References

Module 01 Network Attack and Defense Strategies

1. Ms. Mousami Pawar (Dec 5, 2014), Network Security, from http://www.slideshare.net/mousmip/network-security-fundamental.
2. Internet and Internet Communication(s) (June 2012), from https:// ccdcoe.org/ cycon/ 2012/ workshops/ Internet_ Internet_ Comms.pdf.
3. John E. Canavan, Fundamentals of Network Security, from http://www.askcypert.org/sites/default/files/Canavan_J.E._Fundamentals_of_network_security_(2001)(en)(218s).pdf.
4. DoDD 8570.1: Blue Team, from https://www.sypriselectronics.com/information-security/cyber-security-solutions/computer-network-defense/.
5. Mariusz Stawowski (ISSA Journal October 2007), The Principles of Network Security Design, from http:// www.clico.pl/ services/ Principles_Network_Security_Design.pdf.
6. Diane Teare, Designing for Cisco Internetwork Solutions (DESGN), from http:// portal.aauj.edu/ portal_resources/ downloads/ networking/ designing_network_security_cisco_press.pdf.
7. Types of Networks, http://www.codesandtutorials.com/networking/basics/computer_network-types.php.
8. Department of Defense (March 9, 2001, Support to Computer Network Defense (CND), from https://info.publicintelligence.net/DoD-SupportCND.pdf.
9. Computer Network Defense, from https://www.safaribooksonline.com/library/view/cyber-warfare-2nd/9780124166721/xhtml/CHP011.html.
10. Computer Network Defense (CND), from https://www.techopedia.com/definition/27906/computer-network-defense-cnd.
11. Computer security, from https://en.wikipedia.org/wiki/Computer_security.
12. What is Information Security? From http://demop.com/articles/what-is-information-security.pdf.
13. Computer network operations, from https://en.wikipedia.org/wiki/Computer_network_operations.
14. Margaret Rouse, (Feb 2015), authentication, from http://searchsecurity.techtarget.com/definition/authentication.
15. 5 Core Principles of Information Assurance (May 23, 2011), https://onlinebusinesscertificates.wordpress.com/2011/05/23/5-core-principles-of-information-assurance/.
16. NSA(CSS), Information Assurance, from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
17. Trusted Information Sharing Network for critical infrastructure protection (June 208), from http://www.qcert.org/sites/default/files/public/documents/au-bp-defence_in_depth-eng-2008.pdf.
18. physical security, from http://searchsecurity.techtarget.com/definition/physical-security.
19. Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, Angelos D. Keromytis, A Network Access Control Mechanism Based on Behavior Profiles, from https:// www.cs.columbia.edu/ ~angelos/ Papers/ 2009/acsac09.pdf.
20. Ajay Yadav (April 1, 2013), Network Design: Firewall, IDS/IPS, from http://resources.infosecinstitute.com/network-design-firewall-idsips/.
21. Tony Bradley, Proxy Server, from http://netsecurity.about.com/cs/generalsecurity/g/def_proxy.htm.
22. Hardening (computing), from https://en.wikipedia.org/wiki/Hardening_(computing).
23. Packet Filtering, from https://www.techopedia.com/definition/4038/packet-filtering.
24. Margaret Rouse (March 2001), Common Criteria (CC) for Information Technology Security Evaluation, from http://whatis.techtarget.com/definition/Common-Criteria-CC-for-Information-Technology-Security-Evaluation.
25. GERALD J. POPEK AND CHARLES S. KLINE, Encryption and Secure Computer Networks, from http:// www.cs.swarthmore.edu/ ~newhall/readings/popek.pdf.
26. Feb 2008, Password management, from http://www.infosec.gov.hk/english/technical/files/password.pdf.
27. Deb Shinder (August 28, 2001), Understanding and selecting authentication methods, from http:// www.techrepublic.com/ article/ understanding-and-selecting-authentication-methods/.
28. network configuration management (NCM), from http://searchnetworking.techtarget.com/definition/network-configuration-management.
29. Network Security Audit – Multi platform consolidation with security event correlation, from http://www.enforcive.com/network-security-audit.
30. Frederick M. Avolio (July 2007), Producing your network security policy, from https:// www.watchguard.com /docs /whitepaper /securitypolicy_wp.pdf.
31. STANDARD OPERATING PROCEDURES, http://www.fao.org/docrep/w7295e/w7295e04.htm.
32. Padmavathy Ramesh (July 2002), Business Continuity Planning, from http:// www.tcs.com/ SiteCollectionDocuments/ White%20Papers/Business%20Continuity%20Planning.pdf.
33. Configuration Control, from http://www.chambers.com.au/glossary/configuration_control.php.
34. August 2000, Security Culture: a handbook for activists, from http://www.animalliberationfront.com/ALFront/ELF/sec-handbook.pdf.
35. Jennifer Pfeffer (7/11/2016), What Does a Network Administrator Do? A Behind-the-Scenes Look, from http:// www.rasmussen.edu/ degrees/ technology/ blog/what-does-a-network-administrator-do/.
36. Protecting Data in a Network Environment, from https://docs.oracle.com/cd/B12037_01/network.101/b10777/protnet.htm.

37. Architecture Overview, http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm#wp42293.
38. Nimmy Reichenberg (September 26, 2013), Four Tips for Designing a Secure Network Perimeter, from http://www.securityweek.com/four-tips-designing-secure-network-perimeter.
39. http://secnetpal.com/network-security/prevention-detection-response-trinity-network-securitypart-1.html.
40. http://secnetpal.com/network-security/prevention-detection-response-trinity-network-securitypart-2.html.
41. Incident Response Plan, from http://www.comptechdoc.org/independent/security/policies/incident-response-plan.html.
42. 6 November 2015, Responding to Network Attacks and Security Incidents, from http://www.tech-faq.com/responding-to-network-attacks-and-security-incidents.html.
43. The Difference Between Events, Alerts, and Incidents, from https://danielmiessler.com/study/event-alert-incident/.
44. Vulnerabilities, Threats, and Attacks, from http://www.lovemytool.com/files/vulnerabilities-threats-and-attacks-chapter-one-7.pdf.
45. Responding to Network Attacks and Security Incidents, from http://www.tech-faq.com/responding-to-network-attacks-and-security-incidents.html.
46. Red Team/Blue Team, Capture the Flag, and Treasure Hunt: Teaching Network Security Through Live Exercises, from http://ictf.cs.ucsb.edu/pdfs/2003_WISE_iCTF.pdf.
47. Cyril Onwubiko (13th December 2011), Computer Network Defense Approaches, from http://www.research-series.com/ cyril/ Approaches%20in%20security%20defense.pdf.
48. personal area network (PAN), from http://searchmobilecomputing.techtarget.com/definition/personal-area-network.
49. Personal area network, from https://en.wikipedia.org/wiki/Personal_area_network.
50. The CentOS Project, from https://www.centos.org.
51. Tom Cross (DEC 11, 2012), 5 Key Computer Network Security Challenges For 2013, from http://www.forbes.com/sites/ciocentral/2012/12/11/5-key-computer-network-security-challenges-for-2013/.
52. Vulnerabilities, Threats and attacks, from http://www.lovemytool.com/files/vulnerabilities-threats-and-attacks-chapter-one-7.pdf.
53. CALYPTIX (JUNE 17, 2015), Top 7 Network Attack Types in 2015, from http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/.
54. Global Application & Network Security Report 2014-2015, http://bacher.at/assets/Produkt-Forum/2014-12-Radware-SecurityReport2014-15.pdf.
55. Threat, from https://www.techopedia.com/definition/25263/threat.
56. Rick Lutkus (May 29, 2015), Information Security Threat: Technological Exploits, from http://www.lawtechnologytoday.org/2015/05/information-security-threat-technological-exploits/.
57. Kunal Thakur, Vishal Shirguppi, Justin Francis, Sazia Ali, Packet Sniffing, from http://www.slideshare.net/superfun/packet-sniffers?qid=25ccf028-6c61-4cf2-89a0-e86bd6c8b021&v=qf1&b=&from_search=2.
58. Prabhakar mateti, Port Scanning, from http://www.slideshare.net/amiable_indian/port-scanning?qid=32f4f55f-9818-4622-a2cd-a303d8a45943&v=qf1&b=&from_search=2.
59. CCNA Security: Common Network Attacks, from https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-common-network-attacks/.
60. Choosing an internal domain, from http://www.opendium.com/node/40.
61. CCNA Security: ACLs for Telnet, SNMP and DDOS Attacks, from https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-cisco-routers-and-acls/ccna-security-acls-for-telnet-snmp-and-ddos-attacks/.
62. Angry IP scanner Introduction, from http://angryip.org/documentation/.
63. Review of Engineer's Toolset v10 from SolarWinds, from http:// www.computerperformance.co.uk/ HealthCheck/ engineers_toolset.htm.
64. What is dnswatch.exe?, from http://www.freefixer.com/library/file/dnswatch.exe-107887/.
65. Joseph Caudle (12 February 2015), Top DNS Lookup Tools, from http://blog.dnsimple.com/2015/02/top-dns-lookup-tools/.
66. SpiderFoot from http://www.spiderfoot.net/info/.
67. SpiderFoot –features, from https://whois.arin.net/ui.
68. traceroute, from http://whatis.techtarget.com/definition/traceroute.
69. (24 Jul 2016), CountryTraceRoutev1.27, from http://www.portablefreeware.com/?id=2344.
70. Create network diagrams and export them to Microsoft Visio, from http://www.solarwinds.com/network-topology-mapper.aspx.
71. Facts About Port Scanning, from http://whatismyipaddress.com/port-scan.
72. Port Scanning Techniques, from https://nmap.org/book/man-port-scanning-techniques.html.
73. The Hidden Threat: Misconfigured Access Points, from http://files.moonblink.com/solutionbrief-hidden-threat-of-misconfigured-aps.pdf.
74. Luiz Firmino (5th October 2011), Cyber Defense Misconfigured AP Attack, from http://luizfirmino.blogspot.in/2011/10/misconfigured-ap-attack.html.
75. Unauthorized Association Detected, from http://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/52/wIPS/configuration/guide/msecg_wIPS/msecg_appA_wIPS.html#wp1166633.
76. Luiz Firmino (5th October 2011), Cyber Defense Unauthorized Association, from http://luizfirmino.blogspot.in/2011/10/unauthorized-association.html.
77. Windows 10 Help, from http://windows.microsoft.com/en-in/windows/set-computer-to-computer-adhoc-network#1TC=windows-7.

78. ad-hoc network, from http://searchmobilecomputing.techtarget.com/definition/ad-hoc-network.
79. Know the Risks of Ad Hoc Wireless LANs, from http://www.airdefense.net/eNewsletters/adhoc.shtm.
80. Darren Miller (24 Jan. 2013), The Dangers Of Ad-Hoc Wireless Networking, from http://www.windowsecurity.com/whitepapers/Wireless_Security/Dangers-Ad-Hoc-Wireless-Networking.html.
81. How to Avoid Public WiFi Security Risks, from http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi-risks#.Vq8gXpp97cs.
82. Hot-Spotter Tool Detected (Potential Wireless Phishing), from http://www.cisco.com/c/en/us/td/docs/ wireless/mse/3350/5-2/wIPS/configuration/guide/msecg_wIPS/msecg_appA_wIPS.html#wp1164345.
83. Types of Wireless Network Attacks: Jamming, from http://www.spamlaws.com/jamming-attacks.html.
84. Wireless jamming model, from https://www.nsnam.org/wiki/Wireless_jamming_model.
85. June 14, 2007, Wireless Security, http://fci-h.blogspot.in/2007/06/wireless-security.html.
86. WarDriving, a definition, from http://www.wardriving.com/about.php.
87. Michael Kassner (March 9, 2008), How to prevent automatic association with ad hoc networks, from http://www.techrepublic.com/blog/mobile-enterprise/how-to-prevent-automatic-association-with-ad-hoc-networks/.
88. Wired Equivalent Privacy (WEP), from http://searchsecurity.techtarget.com/definition/Wired-Equivalent-Privacy.
89. MYLES GRAY (JUNE 17, 2015), Scanning for network vulnerabilities using nmap, from http://www.mylesgray.com/security/.
90. scanning-for-network-vulnerabilities-using-nmap/.
91. Eddie Sutton, Footprinting: What is it and How Do You Erase The, from http://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf.
92. Lei Han (April 2006), A Threat Analysis of The Extensible Authentication Protocol, from http://people.scs.carleton.ca/~barbeau/Honours/Lei_Han.pdf.
93. RADIUS Vulnerabilities, http://books.gigatux.nl/mirror/wireless/0321202171/ch13lev1sec4.html.
94. Chameleon WiFi Virus Spreads Like a Cold, from https://blog.malwarebytes.org/online-security/2014/03/chameleon-wifi-virus-spreads-like-a-cold/.
95. darkAudax (20 January 11, 2010), Tutorial: Simple WEP Crack, from http://www.aircrack-ng.org/doku.php?id=simple_wep_crack.
96. Cracking WPA2-PSK Passwords Using Aircrack-Ng, from http://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-psk-passwords-using-aircrack-ng-0148366/.
97. What are crackers and hackers?, from http://www.pctools.com/security-news/crackers-and-hackers/.
98. Threats, Vulnerabilities and Exploits, from https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my.
99. IT Asset, from https://www.techopedia.com/definition/16946/it-asset.
100. Attack Tree Based Information Security Risk Assessment Method Integrating Enterprise Objectives with Vulnerabilities, from https://iajit.org/PDF/vol.10,no.3/13-4356.pdf.
101. Cyberthreat, from https://www.techopedia.com/definition/25263/cyberthreat.
102. Threat types, from https://en.wikipedia.org/wiki/Threat_(computer)#Threats_classification.
103. Types of Security Threats, from http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+1.+Security+Threats/Types+of+Security+Threats/.
104. The Four Primary Types of Network Threats, from http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+1+Understanding+Network+Security+Threats/The+Four+Primary+Types+of+Network+Threats/.
105. Grace Mendzef, CYBERSECURITY THREATS: UNINTENTIONAL VS. INTENTIONAL, Threat Sources, from https://preparis.com/blog/cybersecurity-threats/. Cyber Threat Actors, from https://www.info-savvy.com/cyber-threat-actors/.
106. Forrest Stroud, threat actor, from https://www.webopedia.com/TERM/T/threat-actor.html.
107. Threat, vulnerability, risk – commonly mixed up terms, from https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/.
108. Session Hijacking, from https://g16frameworkmedia.com/session-hijacking/.
109. Zbigniew Banach, What Is Session Hijacking: Your Quick Guide to Session Hijacking Attacks, from https://www.netsparker.com/blog/web-security/session-hijacking/.
110. MITRE ATT&CK, from https://attack.mitre.org/.
111. Welcome to the OWASP Top 10 – 2021, from https://owasp.org/Top10/.
112. Server-Side Request Forgery (SSRF), from https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/.
113. Supply Chain Attacks: Examples and Countermeasures, from https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks.
114. What Is a Supply Chain Attack? from https://www.keepersecurity.com/threats/supply-chain-attack.html.
115. Alexander S. Gillis (Oct 2022), supply chain attack, from https://www.techtarget.com/searchsecurity/definition/supply-chain-attack.
116. Mackenzie Jackson (5 Nov 2021), Supply Chain Attacks: 6 Steps to protect your software supply chain, from https://blog.gitguardian.com/supply-chain-attack-6-steps-to-harden-your-supply-chain/.
117. Baivab Kumar Jena (20 Oct 2023), SolarWinds Attack and All The Details You Need To Know About It, from https://www.simplilearn.com/tutorials/cryptography-tutorial/all-about-solarwinds-attack.

118. Sudip Sengupta (21 Nov 2022), Supply Chain Threats and Vulnerabilities, from https://crashtest-security.com/supply-chain-attack/.
119. Supply Chain Attacks: Definition Examples & History, from https://www.extrahop.com/resources/attacks/supply-chain/.
120. What Is a Supply Chain Attack? from, https://www.proofpoint.com/us/threat-reference/supply-chain-attack#:~:text=In%20a%20hardware%20supply%20chain,access%20to%20the%20corporate%20infrastructure.
121. Sean Ashcroft (18 Oct 2022), Top 10: Supply chain cybersecurity vulnerabilities, from https://supplychaindigital.com/digital-supply-chain/top-10-supply-chain-cybersecurity-vulnerabilities.
122. The Impacts of Supply Chain Attacks, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-a-supply-chain-attack/#:~:text=Supply%20chain%20attacks%20simply%20provide,used%20to%20perform%20data%20breaches.
123. Dec 2020, Supply chain attack, from https://en.wikipedia.org/wiki/Supply_chain_attack.
124. Edward Kost (13 Jul 2023), 11 Ways to Prevent Supply Chain Attacks in 2023, from https://www.upguard.com/blog/how-to-prevent-supply-chain-attacks.
125. 26 oct 2021, 10 extremely effective ways to prevent supply chain attacks, from https://www.cybertalk.org/2021/10/26/10-extremely-effective-ways-to-prevent-supply-chain-attacks/.

Module 02 Administrative Network Security

126. Andy Scott, How to create a good information security policy, from http://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy.
127. Security Policy, https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwj5ou7gj_HJAhUTBo4KHfgiDKYQFggyMAI&url=http%3A%2F%2Fwww.sis.pitt.edu%2Fjjoshi%2FIS2820%2FSpring06%2Fchapter04.doc&usg=AFQjCNF1nWlp6vfAjT3EB49AOqD5AMxYxQ&bvm=bv.110151844,d.c2E.
128. Types of Security Policies, from http://www.helpwithassignment.com/blog/it_security_assignment_help/.
129. Scott hebert, Security policies, from http://slaptijack.com/information-systems/security-policies/.
130. Dec 02, 2004, Understanding physical security: definition, forms, and importance, from http://resources.infosecinstitute.com/physical-security-policy-can-save-company-thousands-dollars/.
131. Password Policy, from http://www.comptechdoc.org/independent/security/policies/password-policy.html.
132. Configuring Password Policies, from https://technet.microsoft.com/en-us/library/dd277399.aspx.
133. Jethro Perkins (16th October 2015), Policy IT User Accounts, from http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/useAccPol.pdf.
134. IS&T Policies: User Accounts Policy, from https://ist.mit.edu/about/policies/useraccounts.
135. POLICY ON USER ACCOUNTS, from http://www.xavier.edu/policy/documents/User-Account-Policy.pdf.
136. March 2007, Network and Server Security Management Policy, from http://www.ryerson.ca/policies/administration/networksecuritypolicy.html.
137. Mike Chapple, Wireless networking security policy, from http://searchsecurity.techtarget.com/tip/Wireless-networking-security-policy.
138. Incident Response Plan, from http://www.comptechdoc.org/independent/security/policies/incident-response-plan.html.
139. incident response plan (IRP), from http://searchsecurity.techtarget.com/definition/incident-response-plan-IRP.
140. Vangie Beal, router, http://www.webopedia.com/TERM/R/router.html.
141. Router Security Policy, from http://www.murchison.net/techno/router-secpol.html.
142. Switch, from http://searchtelecom.techtarget.com/definition/switch.
143. Switch security tips, from http://searchsecurity.techtarget.com/tip/Week-47-Switch-security-tips.
144. ISO/IEC 27033:2010+ Information technology — Security techniques — Network security, from http://www.iso27001security.com/html/27033.html.
145. Information technology — Security techniques — Network security —, from https://webstore.iec.ch/preview/info_isoiec27033-1%7Bed2.0%7Den.pdf.
146. The IT Security Policy Guide, from http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf.
147. Network security policy, http://en.wikipedia.org/wiki/Network_security_policy.
148. Catherine Paquet (Feb 5, 2013), Network Security Concepts and Policies, from http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3.
149. security policy, from http://searchsecurity.techtarget.com/definition/security-policy.
150. Ladan Kianmehr, Deborah Becker, Ali Kamali, Saint Joseph, The importance of written security policy for any network connection from, http://proc.isecon.org/2011/pdf/1774.pdf.
151. Catherine Paquet (Feb 5, 2013), Network Security Concepts and Policies, from http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3.
152. Courtney Hamby (Sep 11, 2013), Advantages Of Network Security, from http://info.avalanwireless.com/blog/bid/334529/Advantages-Of-Network-Security.
153. Rob McMillan (14 April 2014), Information Security Program Management Key Initiative Overview, from https://www.gartner.com/doc/2708617/information-security-program-management-key.

154. Information Security Program September 2013, Management Standard, from http://www.cio.ca.gov/Government/IT_Policy/SIMM5305_A.PDF.
155. Oct 20, 2012, Information Security Management System ISO/IEC 27001 :205 Introduction and Requirements, from http://www.slideshare.net/ControlCase/isms-presentation-oct-202012?qid=b5f12936-0a7d-4dad-9e6e-2b68c654397b&v=&b=&from_search=9.
156. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems, from http://www.iso27001security.com/html/27001.html.
157. Global Information Assurance Certification Paper, from http://www.giac.org/paper/gsec/1811/develop-good-security-policies-tips-assessment-enforcement/102142.
158. Dancho Danchev, Building and Implementing a Successful Information Security Policy, from http:// www.windowsecurity.com/ pages/ security-policy.pdf.
159. end user policy, from http://searchmobilecomputing.techtarget.com/definition/end-user-policy.
160. USER POLICY, from https://www-als.lbl.gov/index.php/user-information/user-policy.html.
161. User account policy, from https://en.wikipedia.org/wiki/User_account_policy.
162. Information Technology (IT) Policy Making, from http://www.catea.gatech.edu/training/ela/policy/index1.php.
163. IT Policies Every Small Business Should Have, from http://www.corpcomputerservices.com/articles/it-policies-small-business.
164. Muhanned Wajahat Rajab (Jun 30, 2013), Physical Security, from http://www.slideshare.net/wajraj/physical-security-presentation-23717721?qid=f4e0b456-8a74-42a7-9543-d03f369c2a72&v=&b=&from_search=2.
165. 30 July 2013, Types of Security Policies in IT, from http://itil-v3-exam-question-papers.blogspot.in/2013/07/types-of-security-policies-in-it.html.
166. Dr. AMAN JANTAN (2012), INFORMATION SECURITY AND ASSURANCE, from http://www.scribd.com/doc/96301211/Eisp-Issp-SysSp#scribd.
167. By Bradley Mitchell, Acceptable Use Policy – AUP, from http://compnetworking.about.com/od/filetransferprotocol/a/aup_use_policy.htm.
168. Acceptable use policy, from http://en.wikipedia.org/wiki/Acceptable_use_policy.
169. Leminhvuong (Oct 13, 2009), Physical Security, from http://www.slideshare.net/leminhvuong/module-10-physical-security?qid=f4e0b456-8a74-42a7-9543-d03f369c2a72&v=&b=&from_search=6.
170. physical security, from http://searchsecurity.techtarget.com/definition/physical-security.
171. Computer security, from https://en.wikipedia.org/wiki/Computer_security.
172. What is Data Validation?, from http://www.wisegeek.com/what-is-data-validation.htm.
173. Session (computer science), from https://en.wikipedia.org/wiki/Session_(computer_science).
174. https://en.wikipedia.org/wiki/Session_(computer_science).
175. Password Policy Guidelines, from http://hitachi-id.com/password-manager/docs/password-policy-guidelines.html.
176. Sarah Granger (05 Jul 2011), The Simplest Security: A Guide To Better Password Practices, from http://www.symantec.com/connect/articles/simplest-security-guide-better-password-practices.
177. April 23, 2009, New Guidelines For Organization-wide Password Management, from http://www.sciencedaily.com/releases/2009/04/090423105900.htm.
178. Jethro Perkins (16th October 2015), Policy IT User Accounts, from https://hipaa.wisc.edu/docs/accountCreation.pdf.
179. Mark Ciampa (Jan 29, 2010), Security+ Guide to Network Security Fundamentals, 3rd Edition, http://www.slideshare.net/itsec/ch08-authentication?qid=30418012-1e73-4fe0-a249-8b397fb3b055&v=&b=&from_search=13.
180. Kristine Buyers (May 8, 2015), Backup and Recovery Tip: Determine Backup Policies and Procedures, from http://go.dewpoint.com/onpoint/determining-backup-policies-and-procedures-for-backup-and-recovery.
181. Data Security, from https://itservices.uchicago.edu/page/data-security.
182. The Unicode Consortium Policy on Handling of Confidential Data, from http://unicode.org/policies/ confidential_data_policy.html.
183. Information Security and Compliance at Michigan Tech, from http://security.mtu.edu.
184. Email Security Policies, from http://ptgmedia.pearsoncmg.com/images/157870264X/samplechapter/157870264X.pdf.
185. What should be in a corporate email security policy?, from https://www.theemaillaundry.com/email-security-policy/.
186. Sample internet usage policy, from http://www.gfi.com/pages/sample-internet-usage-policy.
187. April 15, 2001, Employee Internet Usage Policy, from http://www.workforce.com/articles/employee-internet-usage-policy.
188. Server Documentation Policy, from http://www.comptechdoc.org/independent/security/policies/server-documentation-policy.html.
189. Remote Access Policy, from http://doit.maryland.gov/ support/documents/ security_guidelines/ remote_access_policy.pdf.
190. Remote Access Policy, from http://nics.appstate.edu/standards/remote-access-policy.
191. January 21, 2005, Remote Access Policies Examples, from http://technet.microsoft.com/en-in/library/cc776865(v=ws.10).aspx.
192. Wireless Use Policy, http://www.comptechdoc.org/independent/security/policies/wireless-policy.html.
193. incident response plan, from http://www.comptechdoc.org/independent/security/policies/incident-response-plan.html.
194. incident response plan, (IRP) from http://searchsecurity.techtarget.com/definition/incident-response-plan-IRP.
195. KELLI K. TARALA, Encryption Policy, from http://www.auditscripts.com/samples/encryption-policy.pdf.
196. Fundamentals of Information Systems Security/Access Control Systems, from http://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems.

197. Vincent C. Hu, David F. Ferraiolo, D. Rick Kuhn, Assessment of Access Control Systems, from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf.
198. Controlling Access to a Computer System, http://docs.oracle.com/cd/E23824_01/html/821-1456/concept-28.html.
199. Access control and authentication isn't as simple as setting up user IDs and passwords, from http://searchsecurity.techtarget.com/magazineContent/Interview-CISO-explains-enterprises-access-control-policies.
200. Trunk Port, from https://www.techopedia.com/definition/27008/trunk-port.
201. authentication, authorization, and accounting (AAA), from http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting.
202. Ganesh Dutt Sharma (June 26, 2010), Firewall Security Policy, from http://securityworld.worldiswelcome.com/firewall-security-policy.
203. Do you need an IDS or IPS, or both?, from http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both.
204. Virtual Private Network (VPN) Policy, from www.cpcstech.com/pdf/virtual_private_network.pdf.
205. Virtual Private Network (VPN) Policy, from http://www.iit.edu/ots/virtual_private_network_vpn_policy.shtml.
206. VPN Access & Usage Policy, from http://its.truman.edu/documentation/index.asp?docId=172.
207. Virtual Private Network (VPN) Policy, from http://www.colby.edu/administration_cs/its/policies/its-vpn-policy.cfm.
208. Ivy Wigmore (October 2012), BYOD (bring your own device), from http://whatis.techtarget.com/definition/BYOD-bring-your-own-device.
209. Tony Bradley (Dec 20, 2011), Pros and Cons of Bringing Your Own Device to Work, from http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html.
210. Nov 25, 2002, DMZ Policy and Guidelines, from http://www.nesnip.org/pdf/dmz.pdf.
211. DMZ Guidelines, https://informationsecurity.wustl.edu/information-technology-professionals/policies/dmz-guidelines/.
212. Jonathan Gana KOLO, Umar Suleiman DAUDA, Network Security: Policies and Guidelines for Effective Network Management, from http://ljs.academicdirect.org/A13/007_021.htm.
213. Catherine Paquet (Feb 5, 2013), Network Security Concepts and Policies, from http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3.
214. Role-based Training, from http://www.nativeintelligence.com/ni-role/.
215. Role-based Security Awareness Training, http://www.globallearningsystems.com/products/individual/role-based-training/.
216. Your guide to the Payment Card Industry Data Security Standard (PCI DSS), from http://www.westpac.com.au/docs/pdf/bb/Guide_to_payment_card_indus1.pdf.
217. content filtering (information filtering), from http://searchsecurity.techtarget.com/definition/content-filtering.
218. Electronic Communications Privacy Act (ECPA), from http://epic.org/privacy/ecpa/.
219. Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22., from https://it.ojp.gov/default.aspx?area=privacy&page=1285.
220. The Foreign Intelligence Surveillance Act of 1978 (FISA), from https://it.ojp.gov/default.aspx?area=privacy&page=1286.
221. FISA 101: Why FISA Modernization Amendments Must Be Made Permanent, from http://www.justice.gov/archive/ll/.
222. S. 1927 (110th): Protect America Act of 2007, from https://www.govtrack.us/congress/bills/110/s1927/text.
223. Fact Sheet: The Protect America Act of 2007, from http://georgewbush-whitehouse.archives.gov/news/releases/ 2007/08/20070806-5.html.
224. Protect America Act of 2007, from http://sourcewatch.org/index.php?title=Protect_America_Act_of_2007.
225. Search & Seizure Law, from http://public.getlegal.com/legal-info-center/search-seizure-law/.
226. Understanding Search-and-Seizure Law, from http://www.nolo.com/legal-encyclopedia/search-seizure-criminal-law-30183.html.
227. Rule 41. Search and Seizure, from http://www.law.cornell.edu/rules/frcrmp/rule_41.
228. Search and Seizure and the Fourth Amendment, from http://criminal.findlaw.com/criminal-rights/search-and-seizure-and-the-fourth-amendment.html.
229. What is the Privacy and Civil Liberties Oversight Board?, from http://www.pclob.gov/.
230. Privacy and Civil Liberties Oversight Board, from https://www.federalregister.gov/agencies/privacy-and-civil-liberties-oversight-board.
231. Router Policy, from http://www.murchison.net/techno/router-secpol.html.
232. Internet Usage Policy, from https://www.nibusinessinfo.co.uk/content/sample-acceptable-internet-use-policy.
233. User-Account Policy, from https://technology.cca.edu/policies/user-account-policy.
234. Firewall-Management Policy, from https://www.royalholloway.ac.uk/it/tos/policies/firewallpolicy.pdf.
235. Special-Access Policy, from http://www.utmb.edu/InfoSec/Policies/ps/PS123_SpecialAccess.pdf.
236. Network-Connection Policy, from http://www.salford.ac.uk/__data/assets/pdf_file/0005/516542/Network-Security-and-Connection-Policy.pdf.
237. Business-Partner Policy, from http://www.transfieldservices.com/pdf/Business_Partners_Policy_TMC-0000-LE-0013.pdf.
238. Email Security Policy, from http://www.itdonut.co.uk/it/staff-and-it-training/your-it-policies/sample-email-use-policy.
239. Passwords Policy, from http://www.cpcstech.com/pdf/password_policy.pdf.
240. Physical Security Policy, from http://modgov.sefton.gov.uk/moderngov/Data/Cabinet%20Member%20-%20Corporate%20Services%20(meeting)/20080305/Agenda/Item%2004A.pdf.
241. Server Security Policy, from http://www.cpcstech.com/pdf/server_security_policy.pdf.

242. Information Protection Policy, from http://csirt.org/sample_policies/index.html.
243. Remote Access Policy, from http://csirt.org/sample_policies/index.html.
244. Data Backup Policy, from https://www.royalholloway.ac.uk/it/tos/policies/backuppolicy.pdf.
245. Confidential Data Policy, from https://computing.wayne.edu/docs/u.p.2007-02-confidential-info.pdf.
246. Data Classification Policy, from http://www.awphd.org/presentations/HIPAAproject/reference/DataClassification.pdf.
247. Wireless Network Policy, from http://its.fsu.edu/About-Us/IT-Policies-Guidelines/Wireless-Communications-Policy.
248. Switch Security Policy, from https://www.cs.stonybrook.edu/sites/default/files/wwwfiles/drupalfiles/basicpage/Router_Security_Policy.pdf.
249. Intrusion Detection and Prevention Policy, from http://dii.vermont.gov/sites/dii/files/pdfs/Intrusion-Detection-and-Prevention-Policy.pdf.
250. Personal Device Usage Policy, from http://content.maas360.com/www/images/silverStripe/breakingblackberry/wp_maas360_breaking_blackberry_PersonalDeviceUsage.pdf.
251. Encryption Policy, from http://www.buryccg.nhs.uk/Library/Your_local_nhs/CCGPlanspoliciesandreports/Encryption%20policy%20CCG%201%203%2014.pdf.
252. Information Security Compliance, from https://www.tcdi.com/information-security-compliance-which-regulations/.
253. Compliance and Regulatory Frameworks, from https://www.rapid7.com/fundamentals/compliance-regulatory-frameworks/.
254. Polices Pyramid, from https://policies.vt.edu/assets/policiespyramidnew.pdf.
255. What Are IT Policies, Standards And Guidelines?, from https://binaryblogger.com/2015/02/11/policies-standards-guidelines/.
256. Why Companies Need Compliance, from https://www.blackstratus.com/compliance/.
257. Jeff Battaglino, 7 Hidden Benefits of IT Security Compliance for Your Business, from https://www.cherwell.com/library/blog/it-security-compliance/.
258. Becky Metivier, Cybersecurity Compliance Assessments: It's All About Interpretation, from https://www.tylercybersecurity.com/blog/cybersecurity-compliance-assessments-its-all-about-interpretation.
259. General Data Protection Regulation (GDPR), from https://gdpr-info.eu/.
260. Danny Palmer, What is GDPR?, from https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/.
261. General Data Protection Regulation, from https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.
262. Gramm-Leach-Bliley Act (GLBA), from https://www.ftc.gov.
263. Gramm-Leach-Bliley, from https://dealers-insurance.com/gramm_leach_bliley_act.php.
264. GLBA Compliance Requirements, from https://www.skyhighnetworks.com/cloud-compliance/glba-compliance-require ments/.
265. SANNA NAZIR, Cyber Laws: What Have Different Countries Done To Prevent Cyber Crime?, from https://unbumf.com/cyber-laws-what-have-different-countries-done-to-prevent-cyber-crime/.
266. What is Information System Security Policy (ISSP), from https://www.igi-global.com/dictionary/fear-appeals-threat-perceptions-and-protection-motivation-in-information-systems-security/42993.
267. Nehemiah Mavetera, Investigating Information System Security Policy and AwarenessTraining Programs in South African Organizations, from https://www.academia.edu/2409019/Investigating_Information_System_Security_Policy_and_Awareness_Training_Programs_in_South_African_Organizations.
268. Information Systems Security Policy, from https://www.temenos.com/wp-content/uploads/2019/07/governance-policy-information-systems-security-2019-jul-03.pdf.
269. Yash Tiwari, Security Awareness, from https://resources.infosecinstitute.com/security-awareness/#gref.
270. COREY BLEICH, Top 10 Types of Employee Training Methods, from https://www.edgepointlearning.com/blog/top-10-types-of-employee-training/.
271. MICHAEL MAUGHAN, Employee Security Training Tips: Social Engineering, from https://www.securitymetrics.com/blog/employee-security-training-tips-social-engineering.
272. John McCormick, Take security precautions when an employee leaves the organization, from https://www.techrepublic.com/article/take-security-precautions-when-an-employee-leaves-the-organization/.
273. Employee monitoring, from https://whatis.techtarget.com/definition/employee-monitoring.
274. Lok, Implement policy processes, from https://blog.usecure.io/7-key-steps-to-implement-security-awareness-training#:~:text=IT%20Managers%20often%20need%20to,policy%20or%20encryption%20policy%2C%20etc.
275. Why is ITAM important? https://www.atlassian.com/itsm/it-asset-management#before-the-incident.
276. 15 Sep 2022, what is IT Asset Management? from https://www.electric.ai/blog/what-is-it-asset-management.
277. What is the Purpose of IT Asset Management? from https://www.armis.com/faq/what-is-the-purpose-of-it-asset-management/.
278. 12 Dec 2019, What Is IT Asset Management and Why Is It Important, from https://www.assetinfinity.com/blog/it-asset-management-importance.
279. Andrew Hartwyk (12 Mar 2021), The Importance of IT Asset Management, from https://www.brightfin.com/resources/the-importance-of-it-asset-management/.
280. IT Asset Management (ITAM), from https://www.ivanti.com/glossary/itam.
281. Aratrica Chakraborty(21 Dec 2022), Asset Management: Concept, Importance and Implementation, from https://razorpay.com/blog/business-banking/importance-of-asset-management/.

282. Reda Chouffani, IT asset management (ITAM), from https://www.techtarget.com/searchcio/definition/IT-asset-management-information-technology-asset-management.
283. 01 Oct 2022, What Is IT Asset Management, from https://ca.indeed.com/career-advice/career-development/it-asset-management.
284. Kaye Timonera (04 May 2023) What is IT Asset Management (ITAM), from https://www.esecurityplanet.com/networks/it-asset-management/.
285. What is IT Asset Management (ITAM), from https://www.servicenow.com/products/it-asset-management/what-is-itam.html.
286. Strategic IT Asset Management (ITAM) Software, from https://www.ivanti.com/products/ivanti-neurons-itam.
287. SolarWinds Service Desk, from https://documentation.solarwinds.com/en/success_center/swsd/content/completeguidetoswsd/gs-admin-dashboard-landingpage.htm#link5.
288. Tanya Goncalves (04 Feb 2022), A complete guide to building an asset management policy, from https://www.fiixsoftware.com/blog/asset-management-policy-complete-guide/.
289. Protecting Business Interests with Policies for IT Asset Management, from https://www.ittoolkit.com/articles/asset-management-policies.
290. 07 Mar 2016, ITAM best practice 6: Conduct self-audits, from https://blogs.manageengine.com/help-desk/servicedesk/2016/03/07/itam-best-practice-6-conduct-self-audits.html.
291. Mike Woods (09 August 2023), 50 Best Practices in IT Asset Management, from https://www.camcode.com/blog/50-best-practices-in-it-asset-management/.
292. Joe (16 may 2018), ITAM Basics: 5 Tips for Dealing with SAM Complexity Caused by Decentralized Organizations, from https://www.joetheitguy.com/itam-basics-5-tips-for-dealing-with-sam-complexity-caused-by-decentralized-organizations/.
293. IT Asset Life Cycle Management, from https://www.manageengine.com/products/asset-explorer/it-asset-life-cycle-management.html.
294. Oct 2023, What Is Asset Lifecycle Management, from https://comparesoft.com/asset-management-software/asset-life-cycle/.
295. ITAM (IT Asset Management), from https://itoneinfotech.com/itam-it-asset-management/
296. IT asset management best practices, from https://www.manageengine.com/products/service-desk/it-asset-management/.
297. 27 Jan 2021, What Is Asset Management Compliance, from https://www.assetinfinity.com/blog/asset-management-compliance.
298. 29 Dec 2021, 12 Challenges in IT Asset Management Every Business Needs to Know, from https://blog.airdroid.com/post/12-challenges-in-it-asset-management/.
299. April 2023, Using information technology asset management (ITAM) to enhance cyber security, https://www.cyber.gc.ca/en/using-information-technology-asset-management-itam-enhance-cyber-security-itsm10004.
300. Linda Rosencrance, NICE Framework (National Initiative for Cybersecurity Education Cybersecurity Workforce Framework), from https://www.techtarget.com/searchsecurity/definition/NICE-Framework.
301. ComplianceForge Reference Model: Hierarchical Cybersecurity Governance Framework (HCGF), from https://www.complianceforge.com/grc/hierarchical-cybersecurity-governance-framework/.
302. National Cyber Security Partnership, from https://www.cyberpartnership.org/about-overview.html.
303. 06 March 2023, Cybersecurity Trends And Threats, from https://www.privacy.com.sg/resources/cybersecurity-trends-and-threats/.
304. Security Webinars, from https://www.linkedin.com/advice/0/what-best-sources-resources-staying-updated-latest#:~:text=Security%20Webinars-,Another%20way%20to%20stay%20updated%20on%20the%20latest%20security%20trends,topics%2C%20issues%2C%20and%20solutions
305. 06 Dec 2023, How do you keep up with the latest cybersecurity trends and challenges, from https://www.linkedin.com/advice/3/how-do-you-keep-up-latest-cybersecurity-trends.
306. Sarah Amler (23 March 2023), 8 cybersecurity conferences to attend in 2023, from https://www.techtarget.com/whatis/feature/8-cybersecurity-conferences-to-attend.

Module 03 Technical Network Security

307. Catherine Paquet (5-2-2013), Network Security Concepts and Policies, from http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3.
308. Access Control Principles, from https://www.centos.org/docs/5/html/CDS/ag/8.0/Managing_Access_Control-Access_Control_Principles.html.
309. Ravi S. Sandhu and Pierangela Samarati (September 1994), Access Control: Principles and Practice, from http://www.profsandhu.com/journals/commun/i94ac(org).pdf.
310. Security Controls, from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/s1-sgs-ov-controls.html.
311. Access Control Categories, from https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Categories.
312. Access Control Models, from https://en.wikipedia.org/wiki/Computer_access_control#Access_control_models.
313. 7-6-2016, Access Control Types, from https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Types.
314. Access Control List, from https://en.wikipedia.org/wiki/Access_control_list.
315. Access Control Lists, from https://msdn.microsoft.com/en-us/library/windows/desktop/aa374872(v=vs.85).aspx.
316. Margaret Rouse, Role-based Access control, from http://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC.

317. Attribute based Access control, from https://en.wikipedia.org/wiki/Attribute-based_access_control.
318. 6-5-2015, Attribute based Access control (ABAC)- Overview, from http://csrc.nist.gov/projects/abac/.
319. Sybase Info center archive, from http://infocenter.sybase.com/archive/index.jsp?topic=/com.sybase.help.ase_15.0.sag1/html/sag1/sag1556.htm.
320. Definition of Policy based Access control, from http://hitachi-id.com/concepts/pbac.html.
321. 12-2008, Implement access control systems successfully in your organization from http://searchitchannel.techtarget.com/feature/The-importance-of-access-control.
322. 6-5-2015, Access control policy and implememtnation guides, from http://csrc.nist.gov/projects/ac-policy-igs/index.html.
323. Vincent C. Hu, David F. Ferraiolo, D. Rick Kuhn (September 2006), Assessment of access control systems, from http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf.
324. Margaret Rouse, Network Access control (NAC), from http://searchnetworking.techtarget.com/definition/network-access-control.
325. Network Access control, from https://en.wikipedia.org/wiki/Network_Access_Control#Controversy
326. 2011, Network access control and network security standards, from http://www.ncsi.com/NSAtc11/presentations/tuesday/basics/serrao_hanna.pdf.
327. Andrew plato, Implementing network access control products: how to prep your clients, from http://searchitchannel.techtarget.com/tip/Implementing-network-access-control-products-How-to-prep-your-clients.
328. Deb Shinder (28-8-2001), Understanding and selecting authentication methods, from http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/.
329. Margaret Rouse, Two-factor authentication (2FA), from http://searchsecurity.techtarget.com/definition/two-factor-authentication.
330. Margaret Rouse, Voice recognition (speech recognition), from http://searchcrm.techtarget.com/definition/voice-recognition.
331. Deb Shinder (28-8-2001), Understanding and selecting authentication methods, from http://www.techrepublic.com/article/understanding-and-selecting-authentication-methods/.
332. Hash Function, from https://en.wikipedia.org/wiki/Hash_function.
333. Margaret Rouse, Hashing, from http://searchsqlserver.techtarget.com/definition/hashing.
334. Robert Uzgalis (1995), Advantages of Hash search, from http://www.serve.net/buz/Notes.1st.year/HTML/ C6/rand.016.html.
335. Hashing, from http://www.webopedia.com/TERM/H/hashing.html.
336. Margaret Rouse, Digital Signature, from http://searchsecurity.techtarget.com/definition/digital-signature.
337. 9-1-2014, Non-repudiation and Digital signature, from http://resources.infosecinstitute.com/non-repudiation-digital-signature/.
338. Vangie Beal, Digital Certificate, from http://www.webopedia.com/TERM/D/digital_certificate.html.
339. Margaret Rouse, Digital Certificate, http://searchsecurity.techtarget.com/definition/digital-certificate.
340. Digital Certificates, from https://technet.microsoft.com/en-us/library/cc962029.aspx.
341. PKI Components, from http://www.idcontrol.com/pki-usb-token/pki-components.
342. Proxy server, from http://whatis.techtarget.com/definition/proxy-server.
343. Jason Spidle, Advantages of using Proxy server, from http://science.opposingviews.com/advantages-using-proxy-server-4226.html.
344. Advantages of using Proxy server, from https://www.locaproxy.com/advantages_of_using_a_proxy_server.php.
345. Tor (anonymity network), from https://en.wikipedia.org/wiki/Tor_(anonymity_network).
346. Alan Henry (22-7-2011), Cyberghost VPN is a free anonymous VPN, from http://lifehacker.com/5823586/cyberghost-vpn-is-a-free-anonymous-vpn-that-protects-your-surfing-from-prying-eyes.
347. Honeypot, from https://www.techopedia.com/definition/10278/honeypot.
348. 2-2008, Honeypot security, from http://www.infosec.gov.hk/english/technical/files/honeypots.pdf.
349. Margaret Rouse, Honeypot, from http://searchsecurity.techtarget.com/definition/honey-pot.
350. Honeypot (computing), from https://en.wikipedia.org/wiki/Honeypot_(computing).
351. http://www.thestudymaterial.com/presentation-seminar/electronics-presentation/256-honeypots.html?start=6.
352. Ryan Mohammed (21-3-2001), Sogtware engineering, from http://imps.mcmaster.ca/courses/SE-4C03-01/papers/Mohammed-honeypots.html.
353. Intrusion detection systems from https://en.wikipedia.org/wiki/Intrusion_detection_system.
354. Margaret Rouse, Intrusion detection from http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection.
355. Margaret Rouse, Intrusion prevention, from http://searchsecurity.techtarget.com/definition/intrusion-prevention.
356. Intrusion detection system, from https://en.wikipedia.org/wiki/Intrusion_prevention_system.
357. Packet analyzer, from https://en.wikipedia.org/wiki/Packet_analyzer.
358. Margaret Rouse, Network analyzer, from http://searchnetworking.techtarget.com/definition/network-analyzer.
359. Roger Grimes (28-6-2004), network protocol analyzers, from http://windowsitpro.com/hardware/6-network-protocol-analyzers.
360. Raksha, Sahana, Sai Janaki, Shruti (7-11-2009), Network protocol analyzers, from http://www.slideshare.net/sourav894/network-protocol-analyzer.
361. Wireshark training, from https://www.wireshark.org/docs/.
362. Margaret Rouse, Content filtering (Information filtering) from http://searchsecurity.techtarget.com/definition/content-filtering.

363. Benefits of having a content filtering policy, from http://www.simplewallsoftware.com/tips/benefits-of-having-a-content-filtering-policy.
364. Sandra 4211 (4-5-2010), Security guide to network security fundamentals, from http://www.slideshare.net/Sandra4211/security-guide-to-network-security-fundamentals-third-edition.
365. Margaret Rouse, Pretty good privacy (PGP), from http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy.
366. How PGP works, from http://www.pgpi.org/doc/pgpintro/.
367. Pretty good privacy, from https://en.wikipedia.org/wiki/Pretty_Good_Privacy.
368. S/MIME, from https://en.wikipedia.org/wiki/S/MIME.
369. S/MIME, from http://whatis.techtarget.com/definition/S-MIME-Secure-Multi-Purpose-Internet-Mail-Extensions.
370. De Clerq, Secure mail using SMIME, from http://flylib.com/books/en/2.244.1.106/1/.
371. Competing technologies, from http://ntrg.cs.tcd.ie/mepeirce/Dce/99/ssl/other.htm.
372. Margaret Rouse, S-HTTP from http://searchsoftwarequality.techtarget.com/definition/S-HTTP.
373. Secure Hypertext transfer protocol, from https://en.wikipedia.org/wiki/Secure_Hypertext_Transfer_Protocol.
374. HTTPS, from https://en.wikipedia.org/wiki/HTTPS.
375. Srikanth Ramesh, what is Secure Socket layer (SSL), and how it works, from http://www.gohacking.com/secure-sockets-layer-ssl/.
376. Secure Electronic transaction, from https://en.wikipedia.org/wiki/Secure_Electronic_Transaction.
377. Margaret Rouse, Secure electronic transaction (SET), from http://searchfinancialsecurity.techtarget.com/definition/Secure-Electronic-Transaction.
378. what is SSL?, from http://info.ssl.com/article.aspx?id=10241.
379. What is SSL and what are SSL certificates, from https://www.digicert.com/ssl.htm.
380. Margaret Rouse, Secure Socket layer, from http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL.
381. How does SSL work, from https://www.entrust.com/ssl/.
382. Transport layer security, from https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_record.
383. Paul Szymanski (22-6-2007), What is Transport layer security, from http://www.networkworld.com/article/2303073/lan-wan/what-is-transport-layer-security-protocol-.html.
384. IPsec, from https://en.wikipedia.org/wiki/IPsec#Modes_of_operation.
385. Margaret Rouse, IPsec, from http://searchmidmarketsecurity.techtarget.com/definition/IPsec.
386. Barracuda nextgen firewall F, from https://techlib.barracuda.com/display/bngv52/how+to+create+an+ipsec+vpn+tunnel+between+the+barracuda+ng+firewall+and+a+pfsense+firewall.
387. Point-to-point protocol, from https://en.wikipedia.org/wiki/Point-to-Point_Protocol.
388. Point-to-point protocol, from https://utem-wan.wikispaces.com/Point-to-Point+Protocol+(PPP).
389. Margaret Rouse, PPP (Point-to-point protocol) http://searchnetworking.techtarget.com/definition/PPP.
390. Two factor authentication tools, from http://precisebiometrics.com/two-factor-authentication/.
391. Bell–LaPadula model, from https://www.wikiwand.com/en/Bell%E2%80%93LaPadula_model.
392. Ebru Celikel Cankaya, Bell-LaPadula Confidentiality Model, from https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_773.
393. Biba Model, from https://en.wikipedia.org/wiki/Biba_Model.
394. Nikolai Bezroukov, The Biba Integrity Model, from http://www.softpanorama.org/Access_control/Security_models/biba_model.shtml.
395. Access Control Matrix, from https://en.wikipedia.org/wiki/Access_Control_Matrix.
396. Access control matrix, from from https://tools.ietf.org/html/rfc4949.
397. User Account Control, from https://en.wikipedia.org/wiki/User_Account_Control.
398. User Account Control, from https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview.
399. MAURO HUCULAK, How to take ownership of files and folders on Windows 10, from https://www.windowscentral.com/how-take-ownership-files-and-folders-windows-10.
400. Ryan Puffer, Reduce the number of admins on your servers with Just Enough Administration, from https://techcommunity.microsoft.com/t5/data-center-security/reduce-the-number-of-admins-on-your-servers-with-just-enough/ba-p/372225.
401. Wolfgang Sommergut, Windows Admin Center: Role-based access control, from https://4sysops.com/archives/windows-admin-center-role-based-access-control/.
402. User access options with Windows Admin Center, from https://docs.microsoft.com/en-us/windows-server/manage/windows-admin-center/plan/user-access-options.
403. Margaret Rouse, identity and access management (IAM), from https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system.
404. James A. Martin, What is IAM?, from https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html.
405. Identity and Access Management (IAM), from https://www.polyu.edu.hk/ags/Newsletter/news0911/IAM_details.html.

406. Jagdeep Bhambra, Identity and Access Management, from https://governmenttechnology.blog.gov.uk/2014/06/24/identity-and-access-management/.
407. Enterprise Identity and Access Management, from https://docs.evolveum.com/iam/enterprise-iam/.
408. Network Segmentation Best Practices to Improve Security, from https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/
409. Becky Metivier, The Security Benefits of Network Segmentation, from https://www.tylercybersecurity.com/blog/the-security-benefits-of-network-segmentation.
410. Vangie Beal, Intrusion Detection (IDS) and Prevention (IPS) Systems, from https://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp.
411. Intrusion detection system, from https://en.wikipedia.org/wiki/Intrusion_detection_system.
412. How does an Intrusion Prevention System (IPS) work?, from https://www.quora.com/How-does-an-Intrusion-Prevention-System-IPS-work.
413. Mawardi, How IDS works, from https://steemit.com/education/@mawardi/using-the-management-module-to-build-architecture-and-infrastructure-network-technology-part-2-2017927t22721537z.
414. GURUBARAN S, Intrusion Detection System (IDS) – A Detailed Guide & Working Function -SOC/SIEM, from https://gbhackers.com/ids/.
415. Divyesh aegis, What Are Load balancers And How Do They Work?, from https://hackernoon.com/what-is-load-balancers-and-how-does-it-work-ep1jr3zcw.
416. What Is Load Balancing?, from https://www.nginx.com/resources/glossary/load-balancing/.
417. Security Information and Event Management, from https://www.splunk.com/en_us/siem-security-information-and-event-management.html.
418. Vincent C. Hu, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, from https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf.
419. Authorization Services Guide, from https://www.keycloak.org/docs/latest/authorization_services/index.html.
420. Axiomatics Policy Server, https://immagic.com/eLibrary/ARCHIVES/GENERAL/AXIOM_SE/A080926P.pdf
421. Axiomatics Externalized Dynamic Authorization, from https://axiomatics.com/wp-content/uploads/2021/07/Axiomatics-API-Integration-MuleSoft.pdf.
422. Andrew Froehlich (04 Nov 2022), The 7 core pillars of a zero-trust architecture, from https://www.techtarget.com/searchsecurity/answer/What-are-the-most-important-pillars-of-a-zero-trust-framework.
423. Kapil Raina (17 Apr 2023), Zero Trust Security, from https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/.
424. Scott W. Rose (10 Aug 2020), Zero Trust Architecture, from https://www.nist.gov/publications/zero-trust-architecture.
425. Zero Trust vs. Defense-In-Depth, from https://www.axiad.com/blog/zero-trust-vs-defense-in-depth-whats-the-difference/#:~:text=The%20Differences%20Between%20Zero%20Trust%20and%20Defense%20in%20Depth&text=The%20main%20difference%20is%20that,multiple%20layers%20of%20security%20defenses.
426. Andrew Froehlich (28 Sep 2022), Compare zero trust vs. the principle of least privilege, from https://www.techtarget.com/searchsecurity/answer/Whats-the-difference-between-zero-trust-vs-defense-in-depth.
427. Draksha Sharma, Zero Trust Architecture: What It Is And Best Practices For Implementing It , from https://www.qentelli.com/thought-leadership/insights/zero-trust-architecture-what-it-and-best-practices-implementing-it.
428. 4 Best Practices for Building a Zero Trust Architecture, from https://perception-point.io/guides/zero-trust/what-is-a-zero-trust-architecture-zta/#4_Best_Practices_for_Building_a_Zero_Trust_Architecture.
429. Satish Kumar (27 Jan 2023), Challenge Response Authentication Mechanism (CRAM), from https://www.tutorialspoint.com/challenge-response-authentication-mechanism-cram.
430. Linda Rosencrance (Mar 2021), challenge-response authentication, from https://www.techtarget.com/searchsecurity/definition/challenge-response-system.
431. Chris Odogwu (06 Jul 2023), What Is Challenge Response Authentication Mechanism, from https://www.makeuseof.com/what-is-challenge-response-authentication-mechanism-cram-and-why-is-it-important/#:~:text=Challenge%2Dresponse%20authentication%20mechanism%20(CRAM,measure%20to%20limit%20data%20exposure.
432. Sandra Gittlen, What is identity and access management? Guide to IAM, from https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system.
433. John Turner, The Definitive Guide to Identity and Access Management (IAM), from https://www.strongdm.com/iam.
434. Axiad, 9 Features of a Great Identity and Access Management System, from https://www.axiad.com/blog/features-of-identity-and-access-management-system/.
435. William Jepma (11 may 2022), The Key Features to Look For in an Identity and Access Management Solution, from https://solutionsreview.com/identity-management/features-to-look-for-in-an-identity-and-access-management-solution/.
436. Maile McCarthy (23 May 2023), Identity Access Management (IAM) vs. Privileged Access Management (PAM), from https://www.strongdm.com/blog/iam-vs-pam-difference.
437. Kelsey Kinzer (14 Sep 2021), The Intersection of Identity and Access Management (IAM) and Multi-Factor Authentication (MFA), from https://jumpcloud.com/blog/the-intersection-of-identity-and-access-management-iam-and-multi-factor-authentication-mfa.
438. Andrew Magnusson (05 Oct 2023), What Is Automated Provisioning? Benefits, How It Works & More, from https://www.strongdm.com/blog/automated-provisioning.
439. User provisioning and deprovisioning key benefits, from https://www.onelogin.com/learn/what-is-user-provisioning-and-deprovisioning#:~:text=User%20provisioning%20and%20deprovisioning%20provide,roles%20and%20flexible%20entitlement%20rules.

440. Richard Wang, Privileged Account Management and Identity Access Management, from https://delinea.com/blog/privileged-account-management-and-identity-access-management-same-family-different-strengths.
441. SolarWinds Access Rights Manager, from https://www.solarwinds.com/assets/solarwinds/swdcv2/licensed-products/access-rights-manager/resources/datasheets/arm-datasheet.pdf.
442. Access Rights Manager, from https://www.solarwinds.com/access-rights-manager.
443. SolarWinds Access Rights Manager, from https://crozdesk.com/software/solarwinds-access-rights-manager.
444. Sharon Shea, SOAR (security orchestration, automation and response), from https://www.techtarget.com/searchsecurity/definition/SOAR.
445. What is Security Orchestration Automation and Response (SOAR), from https://www.zenarmor.com/docs/network-security-tutorials/what-is-security-orchestration-automation-and-response-soar.
446. Splunk Security Orchestration, Automation and Response (SOAR), from https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html.

Module 04 Network Perimeter Security

447. Sandiegopchelp (Apr 15, 2008), Firewall Limitations, from http://www.sandiegopchelp.com/firewall-limitations/.
448. Network Security, from http://nptel.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Computer%20networks/pdf/M8L3.pdf.
449. FIREWALLS, from http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf.
450. Donald Stoddard, Thomas M. Thomas (Feb 8, 2012), from http://www.ciscopress.com/articles/article.asp?p=1823359&seqNum=7.
451. Habtamu Abie (January 2000), An Overview of Firewall Technologies, from http://heim.ifi.uio.no/~abie/fwt.pdf.
452. JEFF TYSON, How Firewalls Work, from http://computer.howstuffworks.com/firewall1.htm.
453. How does a firewall work?, from http://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/how-does-a-firewall-work.aspx.
454. An Introduction to Firewalls, from http://www.firewallinformation.com/.
455. Amandeep Kaur (Aug 26, 2010), from http://www.slideshare.net/adkpcte/firewall-presentation.
456. Firewall Defaults and Some Basic Rules, from http://www.downloads.netgear.com/docs/utm_qsgs/utm_fw.pdf.
457. Create A Basic Firewall (Packet Filter) Rule in Astaro Security Gateway (5 Nov 2015), from https://www.sophos.com/en-us/support/knowledgebase/115155.aspx.
458. Understanding Firewall Rules, from https://technet.microsoft.com/en-us/library/cc730951.aspx.
459. Firewall detection, from http://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/firewall-protection.aspx.
460. How Firewalls Protect Your PC, from http://www.comodo.com/resources/home/how-firewalls-work.php.
461. Security News, from http://www.pctools.com/security-news/what-does-a-firewall-do/.
462. G. KRISHNAM RAJU, S. L. N. REDDY, from http://www.scribd.com/doc/22594454/ADVANTAGES-OF-FIREWALL.
463. Vangie Beal, firewall, from http://www.webopedia.com/TERM/F/firewall.html.
464. Michael Cobb, What is firewall?, from http://searchsecurity.techtarget.com/definition/firewall.
465. Firewall Rules, from http://documentation.netgear.com/dg834n/enu/202-10197-02/Firewall.5.4.html.
466. Firewall Rule Basics, from https://doc.pfsense.org/index.php/Firewall_Rule_Basics.
467. Sandra4211 (May 4, 2010), from http://www.slideshare.net/Sandra4211/sygate-personal-firewall-pro-user-guide.
468. Frederic Avolio, from http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html.
469. Per Thorsheim, COMPARING FIREWALL TECHNOLOGIES, from http://www.ittoday.info/AIMS/DSM/84-10-26.pdf.
470. Karen Scarfone, Paul Hoffman, Guidelines on Firewalls and Firewall Policy, from http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf.
471. Network Design: Firewall, IDS/IPS (APRIL 10, 2013), from http://resources.infosecinstitute.com/network-design-firewall-idsips/.
472. Firewall Technologies, from https://www.novell.com/documentation/nbm37/?page=/documentation/nbm37/over/data/ae70nts.html.
473. David W Chadwick, Network Firewall Technologies, from http://www.itsec.gov.cn/webportal/download/2004_network_fw_tech.pdf.
474. Habtamu Abie (January 2000), An Overview of Firewall Technologies, from http://publications.nr.no/directdownload/publications.nr.no/3149/Abie_-_An_overview_of_firewall_technologies.pdf.
475. Network address translation, from http://en.wikipedia.org/wiki/Network_address_translation.
476. Firewall (computing), from http://en.wikipedia.org/wiki/Firewall_(computing).
477. Margaret Rouse, packet filtering, from http://searchnetworking.techtarget.com/definition/packet-filtering.
478. IP Packet Filtering, from https://technet.microsoft.com/en-us/library/cc957881.aspx.
479. Packet Filtering, from http://docstore.mik.ua/orelly/networking_2ndEd/fire/ch08_01.htm.
480. Application firewall, from http://en.wikipedia.org/wiki/Application_firewall.
481. Packet Filtering, from http://www.techopedia.com/definition/4038/packet-filtering.
482. All About Firewalls, from http://firewall-review.narod.ru/circuit_level_gateway.html.

483. Circuit-Level Gateway, from http://www.techopedia.com/definition/24780/circuit-level-gateway.
484. The Network Encyclopedia, from http://www.thenetworkencyclopedia.com/entry/circuit-level-gateway/.
485. All About Firewalls, from http://firewall-review.narod.ru/application_gateway.html.
486. Application Layer Filtering - Firewall Advanced Security, from http://www.internet-computer-security.com/Firewall/Application-Layer-Filtering.html.
487. Deb Shinder (15 Jan. 2004), from http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/Application_Layer_Filtering.html.
488. Rajesh K (June 13, 2009), Network Security, from http://www.excitingip.com/205/what-are-packet-filtering-circuit-level-application-level-and-stateful-multilayer-inspection-firewalls/.
489. Proxy Services, from http://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_03.htm.
490. Network Address Translation, from http://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_04.htm.
491. Virtual Private Networks, from http://docstore.mik.ua/orelly/networking_2ndEd/fire/ch05_05.htm.
492. Firewall Security, from http://www.ipcopper.com/firewalls.htm.
493. Adam Gowdiak (29-30th May 2003), Techniques used for bypassing firewall systems, from https://www.terena.org/activities/tf-csirt/meeting9/gowdiak-bypassing-firewalls.pdf.
494. Evasion (network security), from https://en.wikipedia.org/wiki/Evasion_(network_security).
495. Wing (December 13, 2013), How to Protect Networks against Advanced Evasion Techniques (AET), from http://securitywing.com/how-to-protect-networks-against-advanced-evasion-techniques/.
496. Vijay Kumar (02.17.12), BASIC HACKING SKILLS, from https://basichackingskills.wordpress.com/2012/02/17/firewall-how-it-works/.
497. Olli-Pekka Niemi, Protect Against Advanced Evasion Techniques, from http://www.webtorials.com/main/resource/papers/McAfee/paper29/protect-against-adv-evasion-techniques.pdf.
498. Firewall/IDS Evasion and Spoofing, from https://nmap.org/book/man-bypass-firewalls-ids.html.
499. Ryan Dube (April 23, 2009), How to Bypass Firewalls & Get Into Blocked Websites in School or at Work With FreeProxy (Windows), from http://www.makeuseof.com/tag/how-to-get-into-blocked-websites-in-school-with-freeproxy/.
500. How to Bypass Web Content Filters, from https://www.untangle.com/inside-untangle/bypasswebfilters/.
501. @breenmachine (November 2, 2015), from http://foxglovesecurity.com/2015/11/02/hack-like-the-bad-guys-using-tor-for-firewall-evasion-and-anonymous-remote-access/.
502. Proxy server, https://en.wikipedia.org/wiki/Proxy_server#Bypassing_filters_and_censorship.
503. ICMP tunnel, from https://en.wikipedia.org/wiki/ICMP_tunnel.
504. Daniel Stødle (May 26. 2005), Ping Tunnel, from http://www.mit.edu/afs.new/sipb/user/golem/tmp/ptunnel-0.61.orig/web/.
505. Matt Schulz (August 21, 2009), TUNNELING IP TRAFFIC OVER ICMP, from http://hackaday.com/2009/08/21/tunneling-ip-traffic-over-icmp/.
506. Hans IP over ICMP, http://code.gerade.org/hans/.
507. ICMP Attacks (MARCH 12, 2014), from http://resources.infosecinstitute.com/icmp-attacks/.
508. Configuring ICMP Message Tunneling for MPLS (2012-02-21), from https://www.juniper.net/documentation/en_US/junos12.1/topics/usage-guidelines/mpls-configuring-icmp-message-tunneling.html.
509. Configuring firewalls to prevent users bypassing filtering, from https://community.jisc.ac.uk/library/janet-services-documentation/configuring-firewalls-prevent-users-bypassing-filtering.
510. Firewall Architectures, from http://www.s-w-r.com/Firewall/link5.html.
511. FIREWALL ARCHITECTURES, from http://www.invir.com/int-sec-firearc.html.
512. Bastion host, from http://en.wikipedia.org/wiki/Bastion_host.
513. Firewall Deployment for Multitier Applications (April 2002), from http://zeltser.com/multi-firewall/.
514. FIREWALLS, from http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf.
515. CBK Telecommunications and Network Security - Firewall architecture (Wednesday, 13 June 2012), from http://www.securityarena.com/cissp-crux/74-cbk-telecommunications-and-network-security?start=10.
516. Firewall Design, from http://www.diablotin.com/librairie/networking/firewall/ch04_02.htm.
517. Firewall Facts, from https://sites.google.com/a/pccare.vn/it/security-pages/firewall-facts.
518. Choosing the Right Firewall Topology, from http://www.firewallhelp.com/firewall-topology.html.
519. Firewalls, Tunnels, and Network Intrusion Detection, from http://cs.brown.edu/cgc/net.secbook/se01/handouts/Ch06-Firewalls.pdf.
520. Unified Threat Management, from http://chimera.labs.oreilly.com/books/1234000001633/ch14.html#url_filtering-id1.
521. Krzysztof Zagrodzki (30 Aug. 2002), from http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/A_firewall_in_an_IT_system.html.
522. Compliance Component (06/08/2004), from http://archive.oa.mo.gov/itsd/cio/architecture/domains/security/CC-FirewallEnvironmentsARC.pdf.
523. John Wack, Ken Cutler, Jamie Pole, Guidelines on Firewalls and Firewall Policy, from http://ithandbook.ffiec.gov/media/27459/nis-guide_on_firewall_and_firewall_pol_800_41.pdf.
524. Laura Pelkey (11/16/12), 3 Steps to a Successful Firewall Implementation, from http://blog.icorps.com/bid/138231/3-Steps-to-a-Successful-Firewall-Implementation.

525. Firewall implementation: Perimeter security placement and management, from http://searchnetworking.techtarget.com/tutorial/Firewall-implementation-Perimeter-security-placement-and-management.
526. Edward Tetz, Network Firewall Implementation, from http://www.dummies.com/how-to/content/network-firewall-implementation.html.
527. Firewall implementation, from https://community.jisc.ac.uk/library/advisory-services/firewall-implementation.
528. Scott Hogg (Jul 31, 2011), Firewall Administration Techniques and Tools, from http://www.networkworld.com/article/2220307/cisco-subnet/cisco-subnet-firewall-administration-techniques-and-tools.html.
529. Ethan Banks (11/12/2013), Firewall Administration For Sysadmins: A Primer, from http://www.networkcomputing.com/careers/firewall-administration-sysadmins-primer/2096601244.
530. Ethan Banks (11/12/2013), Firewall Administration For Sysadmins: A Primer, from http://www.networkcomputing.com/networking/firewall-administration-for-sysadmins-part-2-key-concepts/a/d-id/1234542?.
531. Linda Musthaler (Sep 11, 2009), Top 5 best practices for firewall administrators, from http://www.networkworld.com/article/2247110/network-security/top-5-best-practices-for-firewall-administrators.html.
532. basic types of firewalls, from http://www.vesaria.com/Firewall/FAQ/sec19.php.
533. Network packet, from https://en.wikipedia.org/wiki/Network_packet.
534. Firewalls, from http://www.cs.fsu.edu/~breno/CIS-5357/lecture_slides/class16.pdf.
535. John Wack (Fri Feb 3 08:10:14 EST 1995), Little Protection from Insider Attacks, from http://www.vtcif.telstra.com.au/pub/docs/security/800-10/node42.html.
536. Nathan Einwechter (14 Feb 2002), The Enemy Inside the Gates: Preventing and Detecting Insider Attacks, from http://www.symantec.com/connect/articles/enemy-inside-gates-preventing-and-detecting-insider-attacks.
537. Deb Shinder (16 March 2011), Protecting Against Insider Attacks In Todays Network Environments, from http://www.windowsecurity.com/articles-tutorials/misc_network_security/Protecting-Against-Insider-Attacks-Todays-Network-Environments.html.
538. LamonteCristo (Dec 2 '12), How to setup an internal firewall, from http://security.stackexchange.com/questions/17218/how-to-setup-an-internal-firewall.
539. Dave Piscitello, Firewall Best Practices - Egress Traffic Filtering, from http://securityskeptic.typepad.com/the-security-skeptic/firewall-best-practices-egress-traffic-filtering.html.
540. Creating an External Access Rule, from http://wiki.ipfire.org/en/configuration/firewall/rules/external-access.
541. System Administration Guide: Security Services, from http://docs.oracle.com/cd/E19683-01/817-0365/concept-4/index.html.
542. Laura Taylor, (July 5, 2001), Read your firewall logs, from http://www.zdnet.com/news/read-your-firewall-logs/298230.
543. Overview of the Windows Firewall Security Log File in Windows XP (2015-04-29), from http://ecross.mvps.org/howto/overview-of-the-windows-firewall-security-log-file-in-windows-xp.htm.
544. Viewing the Firewall Log, from http://technet.microsoft.com/en-us/library/cc753781(v=ws.10).aspx.
545. Windows Server 2003/2003 R2 Retired Content, from http://technet.microsoft.com/en-us/library/cc787462(v=ws.10).aspx.
546. Anand Sastry, Firewall logging: Telling valid traffic from network 'allows' threats, from http://searchsecurity.techtarget.com/tip/Firewall-logging-Telling-valid-traffic-from-network-allows-threats.
547. Kevin Beaver, from http://searchsecurity.techtarget.com/tip/Firewall-best-practices.
548. Securing Your Network (June 2003), https://msdn.microsoft.com/en-us/library/ff648651.aspx.
549. Manage Firewall Administrators, from https://www.paloaltonetworks.com/documentation/60/pan-os/pan-os/device-management/manage-firewall-administrators.html.
550. Configuring Firewall Rules (January 20, 2009), https://technet.microsoft.com/en-us/library/dd448559(v=ws.10).aspx.
551. Anand Deveriya (Dec 1, 2005), from http://www.ciscopress.com/articles/article.asp?p=426638&seqNum=3.
552. Deb Shinder (July 20, 2007), from http://www.techrepublic.com/blog/10-things/10-ways-to-monitor-what-your-users-are-doing-with-company-computers/.
553. 5 Critical Rules for Firewall Management, from https://www.secureworks.com/resources/wp-five-rules-for-firewall-management.
554. Vinod Mohan, Best Practices for Effective Firewall Management, http://web.swcdn.net/creative/pdf/Whitepapers/Best_Practices_for_Effective_Firewall_Management.pdf.
555. Managing Firewall Access Rules, from http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/fwaccess.html.
556. Skybox Security, from http://www.skyboxsecurity.com/content/skybox-solutions-firewall-management.
557. Intel Security (Aug 30, 2013), Five Website Security Do's and Don'ts for Online Merchants, from https://blogs.mcafee.com/business/five-website-security-dos-and-donts-for-online-merchants/.
558. The Do's and Don'ts of Firewall Audit Tools, from https://www.firemon.com/dos-and-donts-of-firewall-audit-tools/.
559. Neil Roiter (May 10, 2010), from http://www.csoonline.com/article/2125166/network-security/firewall-audit-dos-and-don-ts.html.
560. AdventNet ManageEngine Firewall Analyzer4, from https://download.manageengine.com/products/firewall/FirewallAnalyzer_UserGuide.pdf.
561. AdventNet ManageEngine Firewall Analyzer5, from http://www.zma.com.ar/contenidos/images/image/Firewall%20Analyzer/Documentos/FirewallAnalyzer_UserGuide.pdf.

562. Irene Abezgauz (Thu, 18 Aug 2005), from http://seclists.org/pen-test/2005/Aug/224.
563. Jason Anderson (March 15, 2001), An Analysis of Fragmentation Attacks, from http://www.ouah.org/fragma.html.
564. Tiny Fragment Attack, from https://definedterm.com/a/definition/5029.
565. Tiny Fragment Attack (March 2007), from http://connection.ebscohost.com/c/reference-entries/31670720/tiny-fragment-attack.
566. I. Miller (June 2001), Protection Against a Variant of the Tiny Fragment Attack, from https://tools.ietf.org/html/rfc3128.
567. Chris McNab, Network Security Assessment, from https://www.trustmatta.com/downloads/pdf/Matta_IP_Network_Scanning.pdf.
568. Patrick Harper, Secure IDS deployment best practices, from http://searchitchannel.techtarget.com/tip/Secure-IDS-deployment-best-practices.
569. K.Rajasekhar, B.Sekhar Babu, P.Lakshmi Prasanna, D.R.Lavanya, T.Vamsi Krishna (12-2-11), An Overview of Intrusion Detection System Strategies and Issues, from http://www.ijcst.com/vol24/1/krajasekhar.pdf.
570. IDPS technologies: an overview, from http://ids.nic.in/TNL%20Mar%202009/IDPS/IDPS.pdf.
571. Margaret Rouse, intrusion detection (ID), from http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection.
572. 27-2-2012, What it is Network intrusion detection system?, from http://www.combofix.org/what-it-is-network-intrusion-detection-system.php.
573. How Intrusion Detection Works, from http://www.spamlaws.com/how-intrusion-detection-works.html.
574. Gary C. Kessler (26-7-2016), An Overview of Cryptography, from http://www.garykessler.net/library/crypto.html.
575. How an Intrusion Detection System in a Firewall Works, from http://anti-virus-software-review.toptenreviews.com/how-an-intrusion-detection-system-in-a-firewall-works.html.
576. Deb Shinder (13-7-2005), SolutionBase: Understanding how an intrusion detection system (IDS) works, from http://www.techrepublic.com/article/solutionbase-understanding-how-an-intrusion-detection-system-ids-works/.
577. J. Forlanda (3-2-2010), Intrusion Detection Systems: How They Work, from http://www.brighthub.com/computing/smb-security/articles/65416.aspx
578. Pastore M., Dulaney E, Intrusion Detection Systems, from http://flylib.com/books/en/4.213.1.49/1/.
579. Intrusion detection systems, from https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids-meeting/idsbg.pdf.
580. Fredrik Valeur, Giovanni Vigna, Christopher Kruegel and Richard A. Kemmerer (9-2004), Comprehensive Approach to intrusion detection alert correlation, from http://www.cs.ucsb.edu/~vigna/publications/2004_valeur_vigna_kruegel_kemmerer_TDSC_Correlation.pdf.
581. Nazir Ahmad (17-11-2012), Intrusion detection systems, from http://www.slideshare.net/King8117/intrusion-detection-systems-15218543.
582. Karen Scarfone and Peter Mell (Feb 2007), Guide to Intrusion Detection and Prevention Systems, from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.
583. Przemyslaw Kazienko & Piotr Dorosz (15-6-2004), Intrusion Detection Systems (IDS) Part 2 – Classification, from http://www.windowsecurity.com/articles-tutorials/intrusion_detection/IDS-Part2-Classification-methods-techniques.html.
584. Misuse detection, from http://en.wikipedia.org/wiki/Misuse_detection.
585. Pedro A. Diaz-Gomez, Dean F. Hougen, misuse detection: An Iterative Process vs. A Genetic Algorithm Approach, from http://www.cameron.edu/~pdiaz-go/Iter_GAsMisUseF.pdf.
586. Jie Lin, Intrusion detection, from http://www.csee.wvu.edu/~cukic/CS665/ID.ppt.
587. Kanika, Urmila (June 2013), Security of Network Using Ids and Firewall, from http://www.ijsrp.org/research-paper-0613/ijsrp-p18150.pdf.
588. Shiv Shakti Srivastava, Nitin Gupta, Saurabh Chaturvedi, Saugata Ghosh (2011), A survey on mobile agent based intrusion detection system, from http://www.ijcaonline.org/isdmisc/number6/isdm137.pdf.
589. Saidat Adebukola Onashoga, Adebayo D. Akinde and Adesina Simon Sodiya (2009), A Strategic Review of Existing Mobile Agent Based Intrusion Detection Systems, from http://iisit.org/Vol6/IISITv6p669-682Onashoga623.pdf.
590. http://www.symantec.com/connect/articles/introduction-distributed-intrusion-detection-systems.
591. Nathan Einwechter (8-1-2002), An Introduction To Distributed Intrusion Detection Systems, from http://dspace.thapar.edu:8080/dspace/bitstream/10266/3447/1/601303024_RohiniRajpal.pdf.
592. Julie J.C.H. Ryan (May 2002), Intrusion Detection, from http://www.seas.gwu.edu/~jjchryan/VAIDS051402.pdf.
593. Hudson K., Ruth A. Intrusion Detection Systems, from http://flylib.com/books/en/2.902.1.51/1/.
594. Cisco Network-Based Intrusion detection-Functionalities and Configuration, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/ServerFarmSec_2-1/ServSecDC/8_NIDS.pdf.
595. Intrusion detection system https://en.wikipedia.org/wiki/Intrusion_detection_system.
596. Manish Kumar, Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar (July 2011), Intrusion Detection System - False Positive Alert reduction technique, from http://searchdl.org/public/journals/2011/IJNS/2/3/104.pdf.
597. 20-6-2015, Intrusion Detection, from https://www.owasp.org/index.php/Intrusion_Detection.
598. Kevin Timm (10-9-2001), Strategies to Reduce False Positives and False Negatives in NIDS, from http://www.symantec.com/connect/articles/strategies-reduce-false-positives-and-false-negatives-nids.
599. Tu Hoang Nguyen, JiaWei Luo and Humphrey Waita Njogu (2014), Improving the management of IDS alerts, from http://www.sersc.org/journals/IJSIA/vol8_no3_2014/38.pdf.
600. Intrusion Detection Systems, from http://www.scribd.com/doc/7148986/Intrusion-Detection-Systems.
601. Network Security Center Netsec, from http://www.netsec.org.sa/int_det.htm.

602. Detecting signs of intrusion, from http://ptgmedia.pearsoncmg.com/images/020173723X/samplechapter/allench6.pdf.
603. Vangie Beal (15-7-2005), Intrusion Detection (IDS) and Prevention (IPS) systems, from http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp.
604. Intrusion Detection Systems, from https://www.ischool.utexas.edu/~netsec/ids.html#plac.
605. Riggs C, Network Perimeter Security: Building Defense In-Depth, from http://flylib.com/books/en/4.426.1.54/1/.
606. Intrusion detection system, from http://en.wikipedia.org/wiki/Intrusion_prevention_system.
607. Steve Piper (2011), Intrusion prevention systems for dummies, from http://www.bradreese.com/sourcefire-ips-for-dummies.pdf.
608. What is an intrusion prevention system?, from https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-prevention-system-ips.html.
609. 24-7-2013, How Intrusion Prevention Systems (IPS) Work in firewall?, from http://community.spiceworks.com/topic/362007-how-intrusion-prevention-systems-ips-work-in-firewall.
610. Joel Snyder, Do you need an IDS or IPS, or both?, from http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both.
611. Ron Lepofsky (23-2-2011), Intrusion Detection: Why do I need IDS, IPS or HIDS, from http://www.networkworld.com/article/2228598/security/intrusion-detection--why-do-i-need-ids--ips--or-hids-.html.
612. Ed Sale, Intrusion Detection and Intrusion Prevention, from http://www.cs.unh.edu/~it666/reading_list/Defense/ids_vs_idp.pdf.
613. Jennifer J. Minella, DS vs. IPS: How to know when I you need the technology, from http://searchsecurity.techtarget.com/tip/IDS-vs-IPS-How-to-know-when-you-need-the-technology.
614. 18-3-2014, Security: IDS vs. IPS Explained, from http://www.comparebusinessproducts.com/fyi/ids-vs-ips.
615. R. Kabila (2008), Network Based Intrusion Detection and Prevention Systems in IP-Level security protocols, from http://waset.org/publications/14713/network-based-intrusion-detection-and-prevention-systems-in-ip-level-security-protocols.
616. Jonathan Lister, What are the Advantages & Disadvantages of an Intrusion Detection System?, from http://www.ehow.com/list_7355352_types-systems-available-protect-networks.html.
617. 1-1-2007, Wireless Intrusion Detection and Prevention Systems Analyst Report, from http://www.informationweek.com/whitepaper/Mobility/Wireless-Security/wireless-intrusion-detection-and-prevention-systemwp1213893028282.
618. 6-4-2011, IPS [Intrusion Prevention Systems], from http://bastio1-1-2007, nnux.wordpress.com/2011/04/06/ips-intrustion-prevention-systems-your-2nd-line-of-defense/.
619. d reese (10-9-2008), Intrusion detection systems vs. network behavior analysis: Which do you need?, from http://www.networkworld.com/article/2346145/cisco-subnet/intrusion-detection-systems-vs--network-behavior-analysis--which-do-you-need-.html.
620. Margaret Rouse, network behavior analysis (NBA), from http://searchsecurity.techtarget.com/definition/network-behavior-analysis.
621. Jack TIMOFTE and Praktiker Romania (2007), Securing the Organization with Network Behavior Analysis, from http://www.economyinformatics.ase.ro/content/EN7/JTimofte.pdf.
622. Idps technologies: an overview, from http://ids.nic.in/tnl%20mar%202009/idps/idpsbody.html.
623. 1-3-2007, intrusion detection and prevention systems, from http://seclists.org/isn/2007/Mar/5.
624. Chris Martin, Intrusion Detection and Prevention Systems in the Industrial Automation and Control Systems Environment, from https://ics-cert.us-cert.gov/sites/default/files/pcsf-arc/intrusion_detection_prevention_systems-martin.pdf.
625. Rebecca Bace and Peter Mell (19-8-2001), Intrusion Detection Systems, from http://cryptome.org/sp800-31.htm.
626. Honey pots, honey nets, and padded cell system, from http://www.idc-online.com/technical_references/pdfs/data_communications/Honey_Pots_Honey_Nets_Padded_Cell_system.pdf.
627. What is a honeypot how is it different from a honeynet, from https://www.coursehero.com/file/p1q27mr/What-is-a-honeypot-How-is-it-different-from-a-honeynet-Honey-pots-are-decoy/.
628. Host-Based Firewall, from https://www.techopedia.com/definition/33097/host-based-firewall.
629. IPWITHEASE, NETWORK BASED FIREWALL VS HOST BASED FIREWALL, from https://ipwithease.com/network-based-firewall-vs-host-based-firewall/.
630. How Host-Based Firewalls Work: Architecture, Rules, and Alerts, from https://www.apriorit.com/dev-blog/543-how-host-based-firewall-works.
631. G.S. JACKSON, Host-Based Vs. Network-Based Firewalls, from https://itstillworks.com/hostbased-vs-networkbased-firewalls-2000.html.
632. Using firewalls to separate internal and external networks, from https://help.stonesoft.com/onlinehelp/StoneGate/SMC/6.3.0/GUID-0ED7F859-CF61-4BD9-998F-5F74357B4945.html.
633. William G. Wong, The Advantages of External FirewallsThe Advantages of External Firewalls, from https://www.electronicdesign.com/industrial-automation/article/21805172/the-advantages-of-external-firewalls.
634. Rajesh K, Internal Network Segmentation Firewalls: What are these?, from https://www.excitingip.com/5387/internal-network-segmentation-firewalls-what-are-these/.
635. Internal Firewalls, from http://web.deu.edu.tr/doc/oreily/networking/firewall/ch04_04.htm.
636. Mike Chapple, How to choose a firewall, from https://searchsecurity.techtarget.com/tip/How-to-choose-a-firewall.
637. Understanding and Configuring Snort Rules, from https://blog.rapid7.com/2016/12/09/understanding-and-configuring-snort-rules/.
638. RAJ CHANDEL, How to Detect NMAP Scan Using Snort, from https://www.hackingarticles.in/detect-nmap-scan-using-snort/.

639. Daniel Berman, Integrating Bro IDS with the ELK Stack, from https://logz.io/blog/bro-elk-part-1/.
640. Detecting intruders with Suricata, from https://www.admin-magazine.com/Articles/Detecting-intruders-with-Suricata/(offset)/3.
641. Host Intrusion Detection for Everyone, from https://www.ossec.net/.
642. Log analysis for intrusion detection, from https://dcid.me/oldtexts/log-analysis-for-intrusion-detection.txt.
643. Host-based IDS Solutions, from Wazuh, https://wazuh.com/.
644. About Matt Conran (June 21, 2019) Software-defined perimeter (SDP): A disruptive technology, from https://network-insight.net/2019/06/software-defined-perimeter-sdp-a-disruptive-technology/
645. Karen Mesoznik (February 19, 2019) 5 reasons why you need to replace your VPN with SDP, from https://www.perimeter81.com/blog/network/5-reasons-why-you-need-to-replace-your-vpn-with-sdp/
646. Jason Garbis (2019) It's time for a VPN alternative, https://www.blackhat.com/sponsor-posts/11072019-cyxtera.html
647. Kenny Gill (August 13, 2019) What Is a Software-Defined Perimeter (SDP)?, from https://www.colocationamerica.com/blog/what-is-software-defined-perimeter
648. Abdallah Moubayed (October 9, 2019) Software-Defined Perimeter (SDP): State of the Art Secure Solution for Modern Networks, https://ieeexplore.ieee.org/document/8863736
649. CSA (December 2013) Software Defined Perimeter, https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf
650. Cyxtera, AppGate SDP and Containers–a Perfect Match, https://www.appgate.com/pdfs/AppGate_SDP_with_Containers_Data-Sheet.pdf
651. Eitan Bremler (August 14, 2019) Building zero trust with a software defined perimeter, https://securityboulevard.com/2019/08/building-zero-trust-with-a-software-defined-perimeter-2/
652. SDP Working Group (2016) Software Defined Perimeter for Infrastructure as a Service, https://downloads.cloudsecurityalliance.org/assets/research/sdp/sdp_for_iaas.pdf
653. Michael Howard, Windows Security, from https://kevincurran.org/com535/slides/5c%20Windows%20Security.pdf
654. Wikipedia, Architecture of Windows NT, from https://en.wikipedia.org/wiki/Architecture_of_Windows_NT

Module 05 Endpoint Security-Windows Systems

655. Vangie Beal, The History of Windows Operating Systems, from https://www.webopedia.com/DidYouKnow/Hardware_Software/history_of_microsoft_windows_operating_system.html.
656. Maheshdabade, An Overview on Popular Computer Operating System Families, from https://eitwebguru.com/an-overview-on-popular-computer-operating-system-families/.
657. User mode and kernel modem, from https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode.
658. Windows Programming/User Mode vs Kernel Mode, from https://en.wikibooks.org/wiki/Windows_Programming/User_Mode_vs_Kernel_Mode.
659. Alex Onsman, User Mode vs Kernel Mode, from https://www.tutorialspoint.com/User-Mode-vs-Kernel-Mode.
660. What is the difference between user mode and kernel mode in NT 4.0?, from https://searchwindowsserver.techtarget.com/answer/What-is-the-difference-between-user-mode-and-kernel-mode-in-NT-40.
661. Windows Programming/User Mode vs Kernel Mode, from https://en.wikibooks.org/wiki/Windows_Programming/User_Mode_vs_Kernel_Mode.
662. Architecture of Windows NT, from https://en.wikipedia.org/wiki/Architecture_of_Windows_NT#Kernel_mode.
663. Jeff Atwood, Understanding User and Kernel Mode, from https://blog.codinghorror.com/understanding-user-and-kernel-mode/.
664. What is the difference between the kernel mode and the user mode? Can I do kernel level programming in Windows?, from https://www.quora.com/What-is-the-difference-between-the-kernel-mode-and-the-user-mode-Can-I-do-kernel-level-programming-in-Windows.
665. Security architecture and design, from https://cdn.ttgtmedia.com/searchSecurityChannel/downloads/CISSP+Study+Guide+_Chapt6.pdf.
666. Local Security Authority or LSA basics, from https://searchenterprisedesktop.techtarget.com/answer/Local-Security-Authority-or-LSA-basics.
667. LSA Authentication Model, from https://docs.microsoft.com/en-us/windows/win32/secauthn/lsa-authentication-model.
668. LSA Authentication, from https://docs.microsoft.com/en-us/windows/win32/secauthn/lsa-authentication.
669. LSA Authentication, from https://docs.microsoft.com/en-us/windows/win32/secauthn/lsa-authentication
670. Local Security Authority (LSA), from https://networkencyclopedia.com/local-security-authority-lsa/.
671. An Analysis of Local Security Authority Subsystem, from https://www.ijltet.org/wp-content/uploads/2014/05/9.pdf.
672. Local Security Authority, from https://ldapwiki.com/wiki/Local%20Security%20Authority.
673. Bhanu Sharma, Sandeep Kaur Dhanda, An Analysis of Local Security Authority Subsystem & Extracting Password Using Packet Analyzer - from https://www.ijltet.org/wp-content/uploads/2014/10/16.pdf.
674. Mark E. Russinovich, Alex Ionescu, David A. Solomon, Microsoft Windows Security, from https://www.microsoftpressstore.com/articles/article.aspx?p=2228450&seqNum=2.
675. Windows NT Security, from http://nathanbalon.net/projects/cis450/cis450_NT_security.pdf.

676. Margaret Rouse, Security Accounts Manager (SAM), Kevin Beaver, from https://searchenterprisedesktop.techtarget.com/definition/Security-Accounts-Manager.
677. Kevin Beaver, What you need to know about the Windows Security Accounts Manager, from https://searchenterprisedesktop.techtarget.com/tip/What-you-need-to-know-about-the-Windows-Security-Accounts-Manager.
678. Security Account Manager, from https://www.windows-active-directory.com/windows-security-account-manager.html.
679. Active Directory, from https://searchwindowsserver.techtarget.com/definition/Active-Directory.
680. Introduction of Active Directory Domain Services, from https://www.geeksforgeeks.org/introduction-of-active-directory-domain-services/.
681. Active Directory (AD), from https://www.techopedia.com/definition/25/active-directory.
682. Introduction of Active Directory Domain Services, from https://www.geeksforgeeks.org/introduction-of-active-directory-domain-services/.
683. What are Active Directory Containers? Server Network Infrastructure Components, from https://www.brighthub.com/computing/windows-platform/articles/33795.aspx.
684. Access Control Model, from https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-model.
685. Margaret Rouse, Access control, from https://searchsecurity.techtarget.com/definition/access-control.
686. Parts of the Access Control Model, from https://docs.microsoft.com/en-us/windows/win32/secauthz/access-control-components.
687. Securable Objects, from https://docs.infor.com/help_lsf_cloudsuite_10.0/index.jsp?topic=%2Fcom.lawson.help.serveradmin%2Fcom.lawson.help.lsrdag-c_10.0.x%2FL27051084629050.html.
688. Machine SIDs and Domain SIDs, from https://docs.microsoft.com/en-gb/archive/blogs/aaron_margosis/machine-sids-and-domain-sids.
689. Mandatory Integrity Control, from https://docs.microsoft.com/en-us/windows/win32/secauthz/mandatory-integrity-control.
690. Tony Bradley, Introduction to Windows Integrity Control, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=2e7efdd7-def6-4b1b-995a-e68b328b6f27&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.
691. Service Accounts, from https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/service-accounts.
692. Security auditing, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/security-auditing-overview.
693. Jeff Melnick, Auditing Windows Systems, from https://blog.netwrix.com/2018/08/23/auditing-windows-server/.
694. Windows Server Hardening Checklist, from https://www.netwrix.com/windows_server_hardening_checklist.html.
695. Windows security baselines, from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines.
696. Microsoft Security Compliance Toolkit 1.0, from https://docs.microsof.t.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10.
697. Top 10 Most Important Group Policy Settings for Preventing Security Breaches, Danny Murphy, from https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/.
698. How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases, from https://support.microsoft.com/en-in/help/299656/how-to-prevent-windows-from-storing-a-lan-manager-hash-of-your-passwor.
699. Tim Fisher, How to Open Command Prompt, from https://www.lifewire.com/how-to-open-command-prompt-2618089.
700. Harden Windows 10 - A Security Guide, from https://hardenwindows10forsecurity.com/.
701. Windows 10 Hardening Techniques, from https://resources.infosecinstitute.com/category/certifications-training/securing-windows-ten/windows-10-hardening-techniques/#gref.
702. How to Set a BIOS Password, from https://www.wikihow.com/Set-a-BIOS-Password.
703. Dewayne Adams, How to harden your Windows OS for maximum security, from https://patriot-tech.com/blog/2010/09/22/how-to-harden-your-windows-os-for-maximum-security/.
704. DNSSEC – What Is It and Why Is It Important?, from https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en.
705. Domain Name System Security Extensions, from https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.
706. John Savill, What is Remote Credential Guard?, from https://www.itprotoday.com/windows-8/what-remote-credential-guard.
707. Protect Remote Desktop credentials with Windows Defender Remote Credential Guard, from https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard.
708. Turning Off Network Level Authentication (NLA), from https://kb.parallels.com/en/123661.
709. Configure Network Level Authentication for Remote Desktop Services Connections, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11).
710. Network Level Authentication, from https://en.wikipedia.org/wiki/Network_Level_Authentication.
711. CARLOS PEREZ, Configuring Network Level Authentication for RDP, from https://www.darkoperator.com/blog/2012/3/17/configuring-network-level-authentication-for-rdp.html.
712. Restrict RDP Access by IP Address, from https://support.managed.com/kb/a2499/restrict-rdp-access-by-ip-address.aspx.
713. sengstar2005, How to Setup a Remote Desktop Gateway, from https://turbofuture.com/computers/What-is-Remote-Desktop-Gateway-and-how-to-install.
714. sengstar2005, How to Configure a Remote Desktop Client to Use a Remote Desktop Gateway, from https://turbofuture.com/computers/How-To-Configure-a-Remote-Desktop-Client-To-Use-a-Remote-Desktop-Gateway.

715. Daniel, Setup RD Gateway Role on Windows Server 2012 R2, from https://www.virtuallyboring.com/setup-rd-gateway-role-on-windows-server-2012-r2/.
716. Securing Remote Desktop (RDP) for System Administrators, from https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/securing-remote-desktop-rdp.
717. Restrict RDP Access by IP Address, from https://support.managed.com/kb/a2499/restrict-rdp-access-by-ip-address.aspx.
718. David Richards, Improving Security for your Remote Desktop Connection, from https://www.liquidweb.com/kb/improving-security-for-your-remote-desktop-connection/.
719. Security Primer – Remote Desktop Protocol, from https://www.cisecurity.org/white-papers/security-primer-remote-desktop-protocol/.
720. Remote Desktop (RDP), from https://www.beyondtrust.com/remote-support/features/remote-desktop-protocol-rdp.
721. Matt Ahrens, The Risks of Remote Desktop Access Are Far from Remote, from https://www.darkreading.com/endpoint/the-risks-of-remote-desktop-access-are-far-from-remote/a/d-id/1331820.
722. Securing Remote Desktop (RDP) for System Administrators, from https://security.berkeley.edu/education-awareness/best-practices-how-tos/system-application-security/securing-remote-desktop-rdp.
723. HOW TO SECURE POWERSHELL REMOTING IN A WINDOWS DOMAIN, from https://www.networkadm.in/securing-powershell/.
724. Russell Smith, Enabling Windows 10 Device Guard, from https://www.petri.com/enabling-windows-10-device-guard.
725. Securing PowerShell in the Enterprise, from https://www.cyber.gov.au/sites/default/files/2019-03/Securing_PowerShell.pdf.
726. Russell Smith, Protect Against Malware by Enforcing PowerShell Constrained Language Mode, from https://www.petri.com/protect-malware-enforcing-powershell-constrained-language-mode.
727. Brien Posey, IMPROVE SECURITY WITH POWERSHELL'S CONSTRAINED LANGUAGE MODE, from http://techgenix.com/constrained-language-mode/.
728. 3 Ways to Change PowerShell Execution Policy in Windows 10, from https://www.top-password.com/blog/change-powershell-execution-policy-in-windows-10/.
729. How to Enable or Disable Windows PowerShell 2.0 in Windows 10, from https://www.tenforums.com/tutorials/111654-enable-disable-windows-powershell-2-0-windows-10-a.html.
730. Joey, Windows PowerShell 2.0 Deprecation, from https://devblogs.microsoft.com/powershell/windows-powershell-2-0-deprecation/.
731. Fatima Wahab, How To Disable Windows PowerShell 2.0 On Windows 10, from https://www.addictivetips.com/windows-tips/disable-windows-powershell-2-0-windows-10/.
732. ISIDOROS MONOGIOUDIS, POWERSHELL SECURITY BEST PRACTICES, from https://www.digitalshadows.com/blog-and-research/powershell-security-best-practices/.
733. Matthew Dunwoody, Greater Visibility Through PowerShell Logging, from https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html.
734. Configure PowerShell logging to see PowerShell anomalies in Splunk UBA, from https://docs.splunk.com/Documentation/UBA/4.3.4/GetDataIn/AddPowerShell.
735. Scott Sutherland, PowerShell Remoting Cheatsheet, from https://blog.netspi.com/powershell-remoting-cheatsheet/.
736. Dimitris Tonias, Enable PowerShell Remoting and check if it's enabled, from https://www.dtonias.com/enable-powershell-remoting-check-enabled/.
737. Enable PowerShell remoting, from https://4sysops.com/wiki/enable-powershell-remoting/.
738. PowerShell Remoting Security Considerations, from https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/winrmsecurity?view=powershell-6.
739. How to Use Process Monitor to Track Registry and File System Changes, from https://www.winhelponline.com/blog/process-monitor-track-events-generate-log-file/.
740. Tim Fisher, What Is the Windows Registry?, from https://www.lifewire.com/windows-registry-2625992.
741. Monitoring DNS Traffic for Security Threats, from https://www.eventtracker.com/blog/2016/august/monitoring-dns-traffic-for-security-threats/.
742. Robert Allen, Top 25 Active Directory Security Best Practices, from https://activedirectorypro.com/active-directory-security-best-practices/.
743. Manage Windows Defender Credential Guard, from https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage.
744. Margaret Rouse, Microsoft Windows Defender Credential Guard, from https://searchenterprisedesktop.techtarget.com/definition/Microsoft-Windows-Defender-Credential-Guard.
745. Understanding secure admin workstations, from https://www.microsoft.com/en-us/itshowcase/protecting-high-risk-environments-with-secure-admin-workstations.
746. Best Practices for Securing Administrative Access, from https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.
747. Appendix F: Securing Domain Admins Groups in Active Directory, from https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory.
748. JEA Session Configurations, from https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/session-configurations?view=powershell-6.
749. JEA Role Capabilities, from https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/role-capabilities?view=powershell-6.

750. PATRICK GRUENAUER, PowerShell: Implementing Just-Enough-Administration (JEA), Step-by-Step, from https://sid-500.com/2018/02/11/powershell-implementing-just-enough-administration-jea-step-by-step/.
751. Securing your infrastructure with Just Enough Administration, from https://docs.microsoft.com/en-gb/archive/blogs/miriamxyra/securing-your-infrastructure-with-just-enough-administration.
752. Just Enough Administration, from https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-6.
753. Reduce the number of admins on your servers with Just Enough Administration, from https://docs.microsoft.com/en-gb/archive/blogs/datacentersecurity/jea-overview.
754. Domain Name System Security Extensions, from https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.
755. DNSSEC – What Is It and Why Is It Important?, from https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en.
756. How DNSSEC Works, from https://www.cloudflare.com/dns/dnssec/how-dnssec-works/.
757. Setting Up DNSSEC security, from https://support.google.com/domains/answer/6387342?hl=en.
758. Jarrod, Implement NTLM Blocking in Windows Server 2016, from https://www.rootusers.com/implement-ntlm-blocking-in-windows-server-2016/.
759. Windows Management Instrumentation, from https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page.
760. Sean Wilkins, The IPv6 Transition, from https://www.petri.com/ipv6-transition.
761. IPv6 Tunneling Feature Overview and Configuration Guide, from https://www.alliedtelesis.com/en/documents/ipv6-tunneling-feature-overview-and-configuration-guide.
762. IPv6 Tunneling, from https://www.alliedtelesis.com/sites/default/files/documents/feature-guides/ipv6_tunnel_feature_overview_guide.pdf.
763. IPv6 tunneling, from https://www.ibm.com/support/knowledgecenter/en/ssw_aix_72/network/tcpip_ipv6_tunnel.html.
764. Shawn Brink, Enable or Disable SMB1 File Sharing Protocol in Windows, from https://www.tenforums.com/tutorials/107605-enable-disable-smb1-file-sharing-protocol-windows.html.
765. How to enable/disable SMBv1, SMBv2, and SMBv3 in Windows and Windows Server, from https://www.alibabacloud.com/help/faq-detail/57499.htm.
766. Windows Management Instrumentation, from https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page.
767. SMB security enhancements, from https://docs.microsoft.com/en-us/windows-server/storage/file-server/smb-security.
768. Jarrod, Enable SMB Encryption on SMB Shares, from https://www.rootusers.com/enable-smb-encryption-on-smb-shares/.
769. What is Smart App Control, from https://support.microsoft.com/en-us/topic/what-is-smart-app-control-285ea03d-fa88-4d56-882e-6698afdb7003.
770. Levin Roy, How to Enable Smart App Control in Windows 11, from https://helpdeskgeek.com/windows-11/how-to-enable-and-use-smart-app-control-in-windows-11/#:~:text=Navigate%20to%20Settings%20%3E%20Privacy%20%26%20Security,Control%20settings%20and%20select%20On.
771. Steve whims (15 Dec 2022), Smart App Control, from https://learn.microsoft.com/en-us/windows/apps/develop/smart-app-control/overview.
772. Brink (26 Oct 2022), Enable or Disable Microsoft Vulnerable Driver Blocklist in Windows 11, from https://www.elevenforum.com/t/enable-or-disable-microsoft-vulnerable-driver-blocklist-in-windows-11.10031/.
773. Kazim Ali Alvi (04 Oct 2023), Microsoft Vulnerable Driver Blocklist, from https://windowsreport.com/microsoft-vulnerable-driver-blocklist/.
774. Stella (23 May 2023), How to Enable or Disable Microsoft Vulnerable Driver Blocklist, from https://www.minitool.com/news/enable-disable-microsoft-vulnerable-driver-blocklist.html.
775. 29 Jul 2021, Credentials Protection and Management, from https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/credentials-protection-and-management.
776. Jason Gerend (27 Sep 2023), Configure added LSA protection, from https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection#how-to-disable-lsa-protection.
777. Subhan Zafar (31 Aug 2022), How to close an open port, from https://www.itechtics.com/close-listening-ports/#how-to-close-an-open-port.
778. Shiwangi, How to check what Ports are Open, from https://www.thewindowsclub.com/how-to-check-what-ports-are-open-windows.
779. What is Listening Port, from https://www.javatpoint.com/what-is-listening-port.
780. Windows 10 - Close listening ports, from https://superuser.com/questions/1799397/windows-10-close-listening-ports.
781. Chifundu Kasiya (03 Jan 2023), How to Run the System File Checker (SFC) in Windows, from https://www.makeuseof.com/system-file-checker-sfc-windows/.
782. System integrity, from https://www.ibm.com/docs/en/zos/2.4.0?topic=system-integrity.
783. What is System Integrity Check, from https://www.geeksforgeeks.org/what-is-system-integrity-check/.
784. Vinay Pamnani (25 Oct 2023), Windows Defender System Guard, from https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-system-guard/how-hardware-based-root-of-trust-helps-protect-windows.
785. Vinay Pamnani (31 Jul 2023), System Guard Secure Launch and SMM protection, from https://learn.microsoft.com/en-us/windows/security/hardware-security/system-guard-secure-launch-and-smm-protection.
786. Using System File Checker in Windows, from https://support.microsoft.com/en-us/windows/using-system-file-checker-in-windows-365e0031-36b1-6031-f804-8fd86e0ef4ca.

787. 07 Oct 2016, SFC scannow, from https://answers.microsoft.com/en-us/windows/forum/all/sfc-scannow/bc609315-da1f-4775-812c-695b60477a93.
788. Mauro Huculak (26 Jul 2022), How to use DISM to repair local image on Windows 11, from https://www.windowscentral.com/software-apps/windows-11/how-to-use-dism-to-repair-local-image-on-windows-11.
789. DISM Overview, from https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/what-is-dism?view=windows-11.
790. DISM Image Management Command-Line Options, from https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/dism-image-management-command-line-options-s14?source=recommendations&view=windows-11.
791. DISM Command-Line Options, from https://learn.microsoft.com/en-us/windows-hardware/manufacture/desktop/deployment-image-servicing-and-management--dism--command-line-options?view=windows-11.
792. About OSSEC HIDS, from https://www.ossec.net/about/.
793. Syscheck, from https://www.ossec.net/docs/manual/syscheck/index.html.
794. How to force an immediate syscheck scan, from https://www.ossec.net/docs/docs/manual/syscheck/index.html#how-to-force-an-immediate-syscheck-scan.
795. Syscheck Control, from https://www.ossec.net/docs/docs/programs/syscheck_control.html#syscheck-control.

Module 06 Endpoint Security-Linux Systems

796. Components of Linux System, from https://www.tutorialspoint.com/operating_system/os_linux.
797. What is The Linux Operating System and its Features, from https://www.elprocus.com/linux-operating-system/.
798. What Is Linux?, from https://www.linux.com/what-is-linux/.
799. Introduction to Linux, from https://www.educba.com/introduction-to-linux/.
800. Linux, from https://en.wikipedia.org/wiki/Linux#History.
801. Margaret Rouse, Linux operating system, from https://searchdatacenter.techtarget.com/definition/Linux-operating-system.
802. Linux Architecture, from https://tecadmin.net/tutorial/linux/linux-architecture/.
803. What is The Linux Operating System and its Features, from https://www.elprocus.com/linux-operating-system/.
804. RAJNISH K., What is Linux OS, Its Essential Features & Characteristics?, from http://techtwisted.com/linux-essential-features-and-characteristics/.
805. Joey Sneddon, Ubuntu adds 'Minimal Install' option to installer, from https://www.omgubuntu.co.uk/2018/02/ubuntu-18-04-minimal-install-option.
806. Kiran Kumar, Ubuntu 18.04 LTS Minimal Installation Option Review, from https://www.fosslinux.com/3618/ubuntu-18-04-lts-minimal-installation-option-review.htm.
807. What exactly is GRUB?, from https://askubuntu.com/questions/347203/what-exactly-is-grub.
808. CHRIS HOF, How to Password Protect Ubuntu's Boot Loader, from https://www.howtogeek.com/102009/how-to-password-protect-ubuntus-boot-loader/.
809. Gus Khawaja, LINUX HARDENING: A 15-STEP CHECKLIST FOR A SECURE LINUX SERVER, from https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist.
810. /boot/, from https://en.wikipedia.org/wiki//boot/.
811. What is patch management in Linux?, from https://www.manageengine.com/patch-management/linux-patch-management.html.
812. What is Linux Patch Management?, from https://www.manageengine.com/products/desktop-central/automate-linux-patch-management.html.
813. How to Configure Linux Patch Management, from http://sapphireims.com/howtoguides/How_to_Configure_Linux_Patch_Management.htm.
814. Linux patch management software and strategies, from https://www.gfi.com/patch-management/linux-patch-management.
815. What is Patch Management in Linux, from https://one.comodo.com/blog/patch-management/linux-patch-management.php.
816. Mfillpot, Intro to Slackware Package Management, from https://www.linux.com/training-tutorials/intro-slackware-package-management/.
817. Jack Wallen, Linux 101: Updating Your System, from https://www.linux.com/training-tutorials/linux-101-updating-your-system/.
818. Jarrod, How To Disable USB Storage Devices In Linux, from https://www.rootusers.com/how-to-disable-usb-storage-devices-in-linux/.
819. SHUSAIN, How to disable USB storage on Linux, from https://linuxtechlab.com/disable-usb-storage-linux/.
820. Gus Khawaja, LINUX HARDENING: A 15-STEP CHECKLIST FOR A SECURE LINUX SERVER, from https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist.
821. TOKYONEON, Using Ubuntu as Your Primary OS, Part 1 (Physical Attack Defense), from https://null-byte.wonderhowto.com/how-to/locking-down-linux-using-ubuntu-as-your-primary-os-part-1-physical-attack-defense-0185565/.
822. disable any usb keyboard and mouse, from https://unix.stackexchange.com/questions/274203/disable-any-usb-keyboard-and-mouse.
823. MAGESH MARUTHAMUTHU, How to set password complexity on Linux, from https://www.2daygeek.com/how-to-set-password-complexity-policy-on-linux/.
824. VIEWING PASSWORD POLICIES, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/viewing-the_password_policy.
825. How do I enforce a password complexity policy?, from https://askubuntu.com/questions/244115/how-do-i-enforce-a-password-complexity-policy.

826. Cloudibee, Change password expiry in Linux, from https://www.cloudibee.com/change-password-expiry-in-linux/.
827. Justin Ellingwood, How To Add and Delete Users on an Ubuntu 14.04 VPS, from https://www.digitalocean.com/community/tutorials/how-to-add-and-delete-users-on-an-ubuntu-14-04-vps.
828. How to Stop and Disable Unwanted Services from Linux System, from https://www.tecmint.com/remove-unwanted-services-from-linux/.
829. A Guide to Kill, Pkill and Killall Commands to Terminate a Process in Linux, from https://www.tecmint.com/how-to-kill-a-process-in-linux/.
830. Using Deborphan, from https://sites.google.com/site/easytipsforlinux/using-deborphan.
831. Unusedpkg, from https://github.com/epinna/Unusedpkg.
832. SK, Install Updates And Security Patches Automatically In Ubuntu, from https://www.ostechnix.com/install-updates-security-patches-automatically-ubuntu/.
833. Linux and UNIX Security Features, from https://www.stuartellis.name/articles/unix-security-features/.
834. TOKYONEON, Using Ubuntu as Your Primary OS, Part 3 (Application Hardening & Sandboxing), from https://null-byte.wonderhowto.com/how-to/locking-down-linux-using-ubuntu-as-your-primary-os-part-3-application-hardening-sandboxing-0185710/.
835. cupsd command in Linux with examples, from https://www.geeksforgeeks.org/cupsd-command-in-linux-with-examples/.
836. CUPS, from https://en.wikipedia.org/wiki/CUPS.
837. Rechosen, Disabling unused daemons to speed up your boot sequence, from https://linuxacademy.com/blog/linux/disabling-unused-daemons-to-speed-up-your-boot-sequence/.
838. Daemons, from https://bash.cyberciti.biz/guide/Daemons.
839. Removing the avahi-daemon on Ubuntu, from https://superuser.com/questions/316715/removing-the-avahi-daemon-on-ubuntu.
840. What is a daemon process in Linux?, from https://www.quora.com/What-is-a-daemon-process-in-Linux.
841. Jack Wallen, How to harden Ubuntu Server 16.04 security in five steps, from https://www.techrepublic.com/article/how-to-harden-ubuntu-server-16-04-security-in-five-steps/.
842. How can Shared Memory be dangerous in server environments & how to secure it?, from https://askubuntu.com/questions/346327/how-can-shared-memory-be-dangerous-in-server-environments-how-to-secure-it.
843. What is Shared Memory?, from http://www.csl.mtu.edu/cs4411.ck/www/NOTES/process/shm/what-is-shm.html.
844. Permissions in Linux, from https://www.geeksforgeeks.org/permissions-in-linux/.
845. File Permissions in Linux/Unix with Example, from https://www.guru99.com/file-permissions.html.
846. Ravi Saive, Disable or Enable SSH Root Login and Limit SSH Access in Linux, from https://www.tecmint.com/disable-or-enable-ssh-root-login-and-limit-ssh-access-in-linux/.
847. Matei Cezar, How to Disable SSH Root Login in Linux, from https://www.tecmint.com/disable-ssh-root-login-in-linux/.
848. Prithviraj S., Iptables Tutorial – Securing Ubuntu VPS with Linux Firewall, from https://www.hostinger.in/tutorials/iptables-tutorial#What-is-Iptables-and-How-Does-It-Work.
849. Sun Microsystems, Securing Linux Systems With Host-Based Firewalls Implemented With Linux iptables, from https://www.informit.com/articles/article.aspx?p=169573&seqNum=2.
850. Marin Todorov, 25 Useful IPtable Firewall Rules Every Linux Administrator Should Know, from https://www.tecmint.com/linux-iptables-firewall-rules-examples-commands/.
851. Joseph E. Ikhalia, 4 Best Host-based Firewalls for Your Windows and Linux Devices + Configuration Techniques, from https://medium.com/@IkhaliaJoseph/4-best-host-based-firewalls-for-your-windows-and-linux-devices-configuration-techniques-75203d86360f.
852. Mitchell Anicas, How To Set Up a Firewall with UFW on Ubuntu 14.04, from https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-14-04.
853. Allow or deny a port UFW – Ubuntu, from https://my.esecuredata.com/index.php?/knowledgebase/article/7/allow-or-deny-a-port-ufw-ubuntu.
854. Hazel Virdó, How To Set Up a Firewall with UFW on Ubuntu 16.04, from https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-with-ufw-on-ubuntu-16-04.
855. Elle Krout, How to Configure a Firewall with UFW, from https://www.linode.com/docs/security/firewalls/configure-firewall-with-ufw/.
856. Gabriel Cánepa, How to Secure Network Services Using TCP Wrappers in Linux, from https://www.tecmint.com/secure-linux-tcp-wrappers-hosts-allow-deny-restrict-access/.
857. Vivek Gite, Explain: Linux and UNIX TCP Wrappers – Find Out If a Program Is Compiled With TCP Wrappers, from https://www.cyberciti.biz/faq/tcp-wrappers-hosts-allow-deny-tutorial/.
858. SK, How To Setup Chrooted SFTP In Linux, from https://www.ostechnix.com/setup-chrooted-sftp-linux/.
859. Pradeep Kumar, How to Configure Chroot SFTP Server in Linux, from https://www.linuxtechi.com/configure-chroot-sftp-in-linux/.
860. How to Set Up SFTP Chroot Jail, from https://linuxize.com/post/how-to-set-up-sftp-chroot-jail/.
861. RAMESH NATARAJAN, How to Setup Chroot SFTP in Linux (Allow Only SFTP, not SSH), from https://www.thegeekstuff.com/2012/03/chroot-sftp-setup.
862. Vivek Gite, Linux Kernel /etc/sysctl.conf Security Hardening, from https://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening/.
863. Preston St. Pierre, Securing Linux with Mandatory Access Controls, from https://www.linux.com/news/securing-linux-mandatory-access-controls/.

864. ENHANCING SYSTEM SECURITY WITH A FIREWALL, SELINUX AND SSH LOGINGS, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sec-security.
865. Linux Hardening with OpenSCAP, from https://networksandservers.blogspot.com/2017/03/linux-hardening-with-openscap.html.
866. Secure Boot, from https://docs.espressif.com/projects/esp-idf/en/latest/esp32/security/secure-boot-v1.html#secure-boot-howto.
867. Stan Cox (01 Jun 2022), How to use Secure Boot to validate startup software, from https://www.redhat.com/sysadmin/secure-boot-systemtap#:~:text=Secure%20Boot%20is%20a%20protocol,for%20the%20computer%20to%20load.
868. What is UEFI Secure Boot, from https://wiki.debian.org/SecureBoot#What_is_UEFI_Secure_Boot.3F.
869. RPM Verifying in Package Manager, from https://linuxconcept.com/rpm-verifying-in-package-manager/.
870. Package management, from https://ubuntu.com/server/docs/package-management.
871. Susan Lauber (16 Jun 2020), RPM and GPG: How to verify Linux packages before installing them, from https://www.redhat.com/sysadmin/rpm-gpg-verify-packages.
872. Abhijeet Dahatonde (24 Jan 2023), Package Management In Linux Yum Vs Dnf, from https://www.sevenmentor.com/package-management-in-linux-yum-vs-dnf.
873. 07 Dec 2023, Zypper package manager, from https://documentation.suse.com/smart/systems-management/html/concept-zypper/index.html.
874. Satish Kumar (28 March 2023), 25 Zypper Commands to Manage 'Suse' Linux Package Management, from https://www.tutorialspoint.com/25-zypper-commands-to-manage-suse-linux-package-management#:~:text=Zypper%20is%20command%2Dline%20package,Linux%20package%20management%20system%20efficiently.
875. Enhancing security with the kernel integrity subsystem, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/kernel_administration_guide/enhancing_security_with_the_kernel_integrity_subsystem.
876. Tripwire Enterprise Features, from https://www.tripwire.com/products/tripwire-enterprise.
877. Leveraging the Power of File Integrity Monitoring, from https://www.tripwire.com/resources/datasheets/tripwire-file-integrity-manager.
878. Shiwani Biradar (04 Jun 2021), Enhancing Linux security with Advanced Intrusion Detection Environment (AIDE), from https://www.redhat.com/sysadmin/linux-security-aide.
879. Advanced Intrusion Detection Environment, from https://wiki.archlinux.org/title/AIDE.
880. Hitesh Jethva, How to Install and Use AIDE Advanced Intrusion Detection Environment on CentOS 8, from https://www.howtoforge.com/how-to-install-and-use-aide-on-centos-8/.
881. Rishabh Umrao (24 Aug 202), Advanced Intrusion Detection Environment, from https://ayedaemon.medium.com/advanced-intrusion-detection-environment-c0555693a371.
882. FILE INTEGRITY / HOST-BASED INTRUSION DETECTION SYSTEM, from https://www.la-samhna.de/samhain/.
883. Integrity Measurement Architecture, from https://wiki.gentoo.org/wiki/Integrity_Measurement_Architecture.
884. Command Examples in Linux, from https://www.thegeekdiary.com/inotifywait-command-examples-in-linux/#:~:text=inotifywait%20is%20a%20command%2Dline,file%20being%20created%20or%20deleted.https://docs.kernel.org/admin-guide/filesystem-monitoring.html.
885. Scanning for malware by using Rootkit Hunter in Linux, from https://docs.e2enetworks.com/security/bestpractice/rootkit_hunter.html#:~:text=Rkhunter%20(Rootkit%20Hunter)%20is%20an,strings%20in%20the%20kernel%2C%20etc.

Module 07 Endpoint Security- Mobile Devices

886. Joel Snyder, BYOD, CYOD, COPE, COBO — What Do They Really Mean?, from https://insights.samsung.com/2018/05/09/byod-cyod-cope-cobo-what-do-they-really-mean/.
887. The Advantages & Disadvantages of BYOD, from https://www.1rti.com/the-advantages-disadvantages-of-byod/.
888. What is BYOD?, https://www.itpro.co.uk/strategy/28072/what-is-byod.
889. Craig Donkin, Securing Corporate Mobile Devices, from https://www.contextis.com/en/blog/securing-corporate-mobile-devices.
890. Enterprise Mobility Management: Models and Solutions, from https://www.altexsoft.com/blog/cloud/enterprise-mobility-management-models-and-solutions/.
891. Important Factors to Consider When Implementing A BYOD Policy, from https://www.kmsi.net/important-factors-to-consider-when-implementing-a-byod-policy.
892. Jo Davis, 5 things to consider before implementing BYOD, from https://realbusiness.co.uk/5-things-to-consider-before-implementing-byod/.
893. Choose Your Own Device (CYOD), from https://www.techopedia.com/definition/29909/choose-your-own-device-cyod.
894. BYOD VS. CYOD VS. COPE – HOW TO CHOOSE THE RIGHT ENTERPRISE MOBILITY STRATEGY, from https://www.calero.com/mobility-service-support/byod-vs-cyod-vs-cope-choose-right-enterprise-mobility-strategy/.
895. BRING YOUR OWN DEVICE (BYOD) VS. CHOOSE YOUR OWN DEVICE (CYOD), from http://www.utgjiu.ro/rev_ing/pdf/2018-4/18_S.%20Iovan,%20C.%20Ivanus%20-BRING%20YOUR%20OWN%20DEVICE%20(BYOD)%20VS.%20CHOOSE%20YOUR%20OWN%20DEVICE%20(CYOD).pdf.
896. COPE vs. BYOD vs. CYOD – What's the difference? And how can you protect your data?, from https://www.focus.net.nz/blog/category/general/cope-vs.-byod-vs.-cyod-whats-the-difference-and-how-can-you-protect-your-da.
897. Josh Bouk, CYOD vs BYOD: A Comparative Analysis, from https://www.cassinfo.com/telecom-expense-management-blog/cyod-vs-byod-a-comparative-analysis.

898. Best Practices to Make BYOD, CYOD and COPE Simple and Secure, from https://www.citrix.com/en-in/products/citrix-endpoint-management/byod-best-practices.html.
899. BYOD VS. CYOD VS. COPE – HOW TO CHOOSE THE RIGHT ENTERPRISE MOBILITY STRATEGY, from https://www.calero.com/mobility-service-support/byod-vs-cyod-vs-cope-choose-right-enterprise-mobility-strategy/.
900. LIARNA LA PORTA, What's the best mobile device ownership model for your business?, from https://www.wandera.com/cope-byod-cyod/.
901. Enterprise Mobility Management: Models and Solutions, from https://www.altexsoft.com/blog/cloud/enterprise-mobility-management-models-and-solutions/.
902. What is COPE (Corporate Owned, Personally Enabled)?, from http://ovationwireless.com/cope-corporate-owned-personally-enabled/.
903. Corporately-Owned, Personally-Enabled: When is COPE the Right Mobility Model for Agencies?, from https://www.accenture.com/t20150523T024231__w__/gr-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_14/Accenture-Corporately-Owned-Personally-Enabled-When-COPE-Right-Mobility-Model-Agencies.pdf.
904. Joel Snyder, BYOD, CYOD, COPE, COBO — What Do They Really Mean?, from https://insights.samsung.com/2018/05/09/byod-cyod-cope-cobo-what-do-they-really-mean/.
905. BYOD, CYOD, COPE, COBO — What Do They Really Mean?, from https://www.wired.com/brandlab/2018/06/byod-cyod-cope-cobo-really-mean/.
906. Ines Reinhardt, MOBILITY BASICS PART III: WHAT'S THE DIFFERENCE BETWEEN BYOD, COBO AND COPE?, from https://blog.cortado.com/mobility-basics-whats-the-difference-between-byod-and-cobo/.
907. Sunil Lalvani, Transition from BYOD to COBO, from https://cio.economictimes.indiatimes.com/tech-talk/transition-from-byod-to-cobo/325.
908. How to choose the right mix: BYOD/COPE/CYOD/COBO, from http://docs.media.bitpipe.com/io_12x/io_122848/item_1123795/Mobile%20Device%20Ownership%20-%20How%20to%20Choose%20the%20Right%20Mix.pdf.
909. PANG Jian Hao Jeffrey, CHUA Chee Leong, CHAN Guan Huat, LIM Seh Leng, CHALLENGES IN MOBILE SECURITY, from https://www.dsta.gov.sg/docs/default-source/dsta-about/challenges-in-mobile-security.pdf?sfvrsn=2.
910. Ed Tittel, 7 Enterprise Mobile Security Best Practices, from https://www.cio.com/article/2378779/7-enterprise-mobile-security-best-practices.html.
911. What is Mobile Device Management (MDM)?, from https://www.manageengine.com/products/desktop-central/mobile-device-management-mdm.html.
912. What is MDM (mobile device management)?, from https://www.quora.com/What-is-MDM-mobile-device-management.
913. Bocholt, Everything under control TISLOG MDM - centralized management for your hardware, from https://www.tis-gmbh.de/en/tislog-mdm-mobile-device-management/.
914. Manasdeep, Mobile Device Management (MDM) – Challenges and Solutions, from https://niiconsulting.com/checkmate/2013/07/mobile-device-management-challenges-and-solutions/.
915. What is Mobile Threat Defense?, from https://www.lookout.com/products/mobile-threat-defense/.
916. ROBIN GRAY, What is Mobile Threat Defense (MTD)?, from https://www.wandera.com/what-is-mobile-threat-defense-mtd/.
917. What Is Mobile Threat Defense?, from https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=b211ab8a-0b3b-4177-8a4d-61bfd8a7f1a7&CommunityKey=63909be8-ed89-4445-bfd4-55f7374256ce&tab=librarydocuments.
918. Scott King, Gartner Mobile Threat Defense and Enterprise Mobile Security Guide, from https://blog.zimperium.com/your-guide-to-mobile-threat-defense/.
919. Understanding Unified Endpoint Management, from https://docs.42gears.com/whitepapers/Understanding%20Unified%20Endpoint%20Management.pdf.
920. Mobileiron's Unified endpoint management (UEM), from https://www.mobileiron.com.
921. Ivanti Unified Endpoint Manager, from https://www.ivanti.com/.
922. Workspace ONE Unified Endpoint Management, from https://www.vmware.com.
923. KC Karnes, Mobile App Security Threats and Secure Best Practices, from https://clevertap.com/blog/mobile-app-security/.
924. Prateek Panda, 5 Mobile Application Security Best Practices that Companies Cannot Afford to Miss, from https://www.appknox.com/blog/5-mobile-application-security-best-practices.
925. DAVID ORAGUI, 7 Steps You Should Take to Improve Mobile App Security, from https://themanifest.com/mobile-apps/7-steps-you-should-take-improve-mobile-app-security,
926. 5 Mobile App Security Best Practices you can't Ignore!, from https://www.preludesys.com/mobile-app-security-best-practices/.
927. Vijay Singh, Security Checklist for Mobile Development, from https://hackr.io/blog/mobile-app-security-standards-checklist.
928. Daniel Hein, Mobile Data Security: How to Protect Corporate Data on Mobile Devices, from https://solutionsreview.com/mobile-device-management/mobile-data-security-how-to-protect-corporate-data-on-mobile-devices/.
929. 6 Steps to Rapidly Improve Mobile Data Security, from https://www.imei.com.au/mobile-data-security#datasecurity.
930. 4 Practical Stapes to Safeguard your Mobile Data, from https://www.imei.com.au/mobile-data-security#legislationregulations.
931. Paul Ruggiero and Jon Foote, Cyber Threats to Mobile Phones, from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf.

Module 08 Endpoint Security-IoT Devices

932. Gamal H. Eladl, Technical Requirements for the Application of Internet of Things, from http://ijcsn.org/IJCSN-2017/6-4/Technical-Requirements-for-the-Application-of-Internet-of-Things.pdf.
933. ENTERPRISE INTERNET OF THINGS, from http://www.enterox.com/IoT/articles/enterprise-internet-of-things.htm.
934. Ronak Patel, IoT for Business Enterprises: Everything You Need to Know, from https://dzone.com/articles/iot-for-business-enterprises-attributes-challenges.
935. Jonathan Greig, IoT device security: 5 tips for enterprises, from https://www.techrepublic.com/article/iot-device-security-5-tips-for-enterprises/.
936. Zeus Kerravala, NETWORK INTELLIGENCE, from https://www.networkworld.com/article/3336269/build-security-into-your-iot-plan-or-risk-attack.html.
937. Vishruta Rudresh, IoT Security Reference Architecture, from https://cdn2.hubspot.net/hubfs/2539908/Whitepapers/IoT%20Security%20Reference%20Architecture_September-2018.pdf.
938. Steven Lerner, 12 IoT Security Challenges And How to Address Them in the Enterprise, from https://www.enterprisedigi.com/iot/articles/iot-security-challenges.
939. Andrey Nikishin, What is a secure internet of things?, from https://os.kaspersky.com/2018/05/31/what-is-a-secure-internet-of-things/.
940. IOT MATTERS, DDoS attacks using IoT devices follow The Manchurian Candidate model, from https://www.networkworld.com/article/3128372/ddos-attacks-using-iot-devices-follow-the-manchurian-candidate-model.html.
941. Lucian Constantin, How to Protect Your Home Router from Attacks, from https://www.vice.com/en_us/article/9kn3g7/how-to-protect-your-home-router-from-attacks.
942. Beyond Three Dumb Routers, from https://www.pcwrt.com/2018/06/beyond-three-dumb-routers/.
943. Using VLANs for Network Isolation, from https://www.routersecurity.org/vlan.php.
944. 9 Best Bandwidth Monitor and Network Usage Monitoring Tools, from https://www.dnsstuff.com/bandwidth-monitor.
945. Cloud IoT Core, from https://cloud.google.com/iot-core.
946. NICK CARSTENSEN, IMPROVING IOT SECURITY WITH LOG MANAGEMENT, from https://www.graylog.org/post/improving-iot-security-with-log-management.
947. David Strom, 9 ways to improve IoT device security, from https://www.hpe.com/us/en/insights/articles/9-ways-to-make-iot-devices-more-secure-1701.html.
948. Viewing device logs, from https://cloud.google.com/iot/docs/how-tos/device-logs.
949. Calum Barnes, Check up on your remote fleet: Cloud IoT now makes Device Activity Logging generally available, from https://cloud.google.com/blog/products/iot-devices/cloud-iot-now-makes-device-activity-logging-generally-available.
950. Wenyuan Xu, Ke Ma, W. Trappe, Yanyong Zhang, Jamming sensor networks: Attack and defense strategies, from https://www.researchgate.net/publication/3283057_Jamming_sensor_networks_Attack_and_defense_strategies.
951. Alex Grizhnevich, IoT architecture: building blocks and how they work, from https://www.scnsoft.com/blog/iot-architecture-in-a-nutshell-and-how-it-works.
952. The Layers of IoT, from https://www.iotsense.io/blog/the-layers-of-iot/.
953. IoT Ecosystem, from https://www.educba.com/iot-ecosystem/.
954. What Is the Internet of Things Ecosystem?, from https://etma.org/what-is-iot-ecosystem/.
955. NATALLIA SAKOVICH, Internet of Things (IoT) Protocols and Connectivity Options: An Overview, from https://www.sam-solutions.com/blog/internet-of-things-iot-protocols-and-connectivity-options-an-overview/.
956. Internet of Things (IoT) Networks, from https://www.sureuniversal.com/the-types-of-iot-networks-the-role-they-play/.
957. Protocols of IoT, from https://www.iotsense.io/blog/protocols-of-iot/.
958. Uwazie Emmanuel Chinanu, Onoja Emmanuel Oche, Joy O. Okah-Edemoh, Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures, from https://arpgweb.com/pdf-files/sr4(10)80-89.pdf.
959. Murat Aydos, Yılmaz Vural, Adem Tekerek, Assessing risks and threats with layered approach to Internet of Things security, from https://journals.sagepub.com/doi/full/10.1177/0020294019837991.
960. Hezam Akram Abdul-Ghani, Dimitri Konstantas, Mohammed Mahyoub, A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model, from https://thesai.org/Downloads/Volume9No3/Paper_49-A_Comprehensive_IoT_Attacks_Survey.pdf.
961. Ehsan ul Haq, Tariq Aziz Rao, Security Challenges Facing IoT Layers and its Protective Measures, from https://www.researchgate.net/publication/323892938_Security_Challenges_Facing_IoT_Layers_and_its_Protective_Measures.
962. OWASP Top 10 IoT Vulnerabilities Solutions, from https://www.owasp.org.
963. Working Groups, from https://aioti-space.org/working-groups/.
964. Working Group, from https://aioti.eu/working-groups/.
965. Bipartisan Legislation to Improve Cybersecurity of Internet-of-Things Devices Introduced in Senate & House, from https://www.warner.senate.gov/public/index.cfm/2019/3/bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-devices-introduced-in-senate-house.
966. Internet of Things Cybersecurity Improvement Act of 2019, from https://www.govtrack.us/congress/bills/116/s734/summary.
967. Internet of Things Cybersecurity Improvement Act of 2019 IoT Cybersecurity Improvement Act of 2019, from https://www.billtrack50.com/BillDetail/1101863.

968. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT), from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.
969. IoT Security Guidelines for Network Operators, from https://www.gsma.com/iot/iot-security-guidelines-for-network-operators/.
970. IoT Security Guidelines for Network Operators, from https://www.gsma.com/iot/wp-content/uploads/2019/10/CLP.14-v2.1.pdf.
971. Sunetra Chakravarti, What threat does IoT pose to printers' kit?, from https://www.printweek.com/features/article/what-threat-does-iot-pose-to-printers-kit.
972. Chris Goetting, Security Hazards Of The IoT: Your Printer Is A Vulnerability Minefield, from https://hothardware.com/reviews/navigating-the-printer-security-minefield.
973. Kelly Sheridan, Printers: The Weak Link in Enterprise Security, from https://www.darkreading.com/endpoint/printers-the-weak-link-in-enterprise-security/d/d-id/1330127.
974. Steve Zurier, How Hackers Hit Printers, from https://www.darkreading.com/risk/how-hackers-hit-printers-/d/d-id/1332715.
975. Nate Beach-Westmoreland, PRINTER VULNERABILITIES LEAVE COMPANIES AT RISK, from https://www.boozallen.com/c/insight/blog/printer-vulnerabilities-leave-companies-at-risk.html.
976. A Comprehensive Approach To Printer Security, from https://www.office.xerox.com/latest/XOGFS-62U.PDF.
977. Smart thermostat, from https://en.wikipedia.org/wiki/Smart_thermostat#Issues_with_programmable_thermostats.
978. How To: Secure Your Smart Thermostat for Added Privacy, from https://greycoder.com/how-to-secure-your-wifi-thermostat-for-added-privacy/.
979. Abiodun Awojobi, Hsia-Ching Chang, Security and Privacy Issues with Smart Thermostats – A First Look, from https://digital.library.unt.edu/ark:/67531/metadc1036560/m2/1/high_res_d/Biodun_Awojobi.pdf.
980. Fatemeh Halim, Salman Yussof and Mohd. Ezanee Rusli, Cyber Security Issues in Smart Meter and Their Solutions, from http://paper.ijcsns.org/07_book/201803/20180314.pdf.
981. Margaret Rouse, smart bulb (smart light bulb), from https://internetofthingsagenda.techtarget.com/definition/smart-bulb-smart-light-bulb.
982. JAMES GELINAS, Beware: Smart light bulbs could expose you to cyberattacks, Beware: Smart light bulbs could expose you to cyberattacks, from https://www.komando.com/security-privacy/smart-light-bulbs-hacking-risk/609437/.
983. Brian Scriber, But it's Just a Light Bulb, Does it Need All This Security?, from https://www.cablelabs.com/just-lightbulb-need-security.
984. Internet of Things (IoT) security: 9 ways you can help protect yourself, from https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html.
985. 12 tips to help secure your smart home and IoT devices, from https://us.norton.com/internetsecurity-iot-smart-home-security-core.html.
986. Jacob Arellano, Best Practices for Securing IoT Devices, from https://www.verypossible.com/blog/best-practices-for-securing-iot-devices.
987. Dean Hamilton, Best practices for IoT security, from https://www.networkworld.com/article/3266375/best-practices-for-iot-security.html.
988. George Corser, INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES, from https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.
989. Conner Forrest, Ten best practices for securing the Internet of Things in your organization, from https://www.zdnet.com/article/ten-best-practices-for-securing-the-internet-of-things-in-your-organization/.

Module 09 Administrative Application Security

990. How to Block an Application or .EXE from Running in Windows, from https://www.wikihow.com/Block-an-Application-or-.EXE-from-Running-in-Windows.
991. WALTER GLENN, How to Block (or Allow) Certain Applications for Users in Windows, from https://www.howtogeek.com/howto/8739/restrict-users-to-run-only-specified-programs-in-windows-7/.
992. Anand Khanse, Block users from installing or running programs in Windows 10, from https://www.thewindowsclub.com/how-to-prevent-users-from-installing-programs-in-windows-7.
993. Danny Murphy, Top 10 Most Important Group Policy Settings for Preventing Security Breaches, from https://www.lepide.com/blog/top-10-most-important-group-policy-settings-for-preventing-security-breaches/.
994. Detect and block potentially unwanted applications, from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/detect-block-potentially-unwanted-apps-windows-defender-antivirus.
995. Shawn Brink, How to Enable or Disable Windows Defender PUA Protection in Windows 10, from https://www.tenforums.com/tutorials/32236-enable-disable-windows-defender-pua-protection-windows-10-a.html
996. Application Security, from https://www.techopedia.com/definition/13567/application-security.
997. PHILIPP REISINGER, Application Whitelisting, from https://prime.sba-research.org/wp-content/uploads/2016/09/sbaPRIME_WP_Application-Whitelisting.pdf.
998. Byron Hynes, Defense in Depth: How Application Whitelisting Can Increase Your Desktop Security, from https://www.faronics.com/assets/AE_WP_ApplicationWhitelisting_EN.pdf.
999. Key Benefits of Application Whitelisting and How to Achieve Them, from https://informationsecurity.report/Resources/Whitepapers/1c85dda9-96c8-449a-affd-cc8ef4f07d55_Key%20Benefits%20of%20Application%20White-Listing%20and%20How%20to%20Achieve%20Them.pdf.
1000. Advantages of Application Whitelisting software, from https://promisecholdings.wordpress.com/2016/12/09/advantages-of-application-whitelisting-software/.

References

1001. Nate Lord, What is Application Whitelisting? An Application Whitelisting Definition, from https://digitalguardian.com/blog/what-application-whitelisting-application-whitelisting-definition.
1002. Blacklist (computing), from https://en.wikipedia.org/wiki/Blacklist_(computing).
1003. Margaret Rouse, application blacklisting, from https://searchsecurity.techtarget.com/definition/application-blacklisting.
1004. Blacklisting vs. Whitelisting, from https://consoltech.com/blog/blacklisting-vs-whitelisting/.
1005. Lawrence Abrams, How to create an Application Whitelist Policy in Windows, from https://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/#whitelist.
1006. Work with Software Restriction Policies Rules, from https://docs.microsoft.com/en-us/windows-server/identity/software-restriction-policies/work-with-software-restriction-policies-rules#BKMK_Path_Rules.
1007. Software Restriction Policies, from https://www.free-online-training-courses.com/software-restriction-policies/.
1008. How To use Software Restriction Policies in Windows Server 2003, from https://support.microsoft.com/en-us/help/324036/how-to-use-software-restriction-policies-in-windows-server-2003.
1009. Brien Posey, Implementing software restriction policies, from https://searchnetworking.techtarget.com/tip/Implementing-software-restriction-policies.
1010. AppLocker, from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview.
1011. Use AppLocker to create a Windows 10 kiosk that runs multiple apps, from https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-applocker.
1012. Shawn Brink, How to Use AppLocker to Allow or Block Executable Files from Running in Windows 10, from https://www.tenforums.com/tutorials/124008-use-applocker-allow-block-executable-files-windows-10-a.html.
1013. How to configure AppLocker Group Policy to prevent software from running, from https://social.technet.microsoft.com/wiki/contents/articles/5211.how-to-configure-applocker-group-policy-to-prevent-software-from-running.aspx.
1014. McAfee Application and Change Control, from https://www.mcafee.com/enterprise/en-in/products/application-change-control.html.
1015. Add certificates, from https://docs.mcafee.com/bundle/application-control-8.1.0-windows-product-guide-unmanaged/page/GUID-4E2D850F-B70C-46C7-892A-F124D2B4D5E4.html.
1016. Create the whitelist, from https://docs.mcafee.com/bundle/application-control-8.1.0-windows-product-guide-unmanaged/page/GUID-55E0A55B-21EC-4948-9010-A2C9FA3B94C8.html.
1017. McAfee Application Control 7.0: New Threat Intelligence-Based Approaches and Strategies, from https://www.mcafee.com/blogs/enterprise/security-operations/application-control-7-0/.
1018. McAfee Application Control: Putting Your Whitelist on Autopilot, from https://www.mcafee.com/blogs/enterprise/cloud-security/mcafee-application-control-putting-whitelist-autopilot/.
1019. Block Executable, from https://www.manageengine.com/products/desktop-central/help/inventory/block_executables.html.
1020. Configure Prohibited Software, from https://www.manageengine.com/products/desktop-central/help/inventory/configure_prohibited_software.html.
1021. Remove Blacklisted Software Automatically, from https://www.manageengine.com/products/desktop-central/prohibited-software.html.
1022. Software Inventory Reports, from https://www.manageengine.com/products/desktop-central/help/inventory/viewing_software_inventory_reports.html#Prohibited-Software.
1023. Block Executable, from https://www.manageengine.com/products/desktop-central/help/inventory/block_executables.html#Block_using_Path_Rule.
1024. Remove Blacklisted Software Automatically, from https://www.manageengine.com/products/desktop-central/prohibited-software.html.
1025. Shawn Brink, How to Enable or Disable Windows Defender PUA Protection in Windows 10, from https://www.tenforums.com/tutorials/32236-enable-disable-windows-defender-pua-protection-windows-10-a.html.
1026. MARTIN PRAMATAROV, Whitelisting vs Blacklisting, preventing or reacting, from https://www.cloudns.net/blog/whitelisting-vs-blacklisting-preventing-reacting/.
1027. Sandboxing, from https://techterms.com/definition/sandboxing.
1028. Ilan Dray, And today… What is SANDBOX?, from https://medium.com/@ilandray/and-today-what-is-sandbox-4e55a5a6733b.
1029. Effective Android Security, from https://orhanobut.github.io/effective-android-security/.
1030. About App Sandbox, from https://developer.apple.com/library/archive/documentation/Security/Conceptual/AppSandboxDesignGuide/AboutAppSandbox/AboutAppSandbox.html.
1031. ALEXANDER FOX, What is macOS Sandboxing and Why Does It Exist?, from https://www.applegazette.com/mac/what-is-macos-sandboxing-and-why-does-it-exist/.
1032. Fahmida Y. Rashid, Application Sandboxes Won't Stop Advanced Attacks: Research, from https://www.securityweek.com/application-sandboxes-wont-stop-advanced-attacks-research.
1033. CHRIS HOFFMAN, from Sandboxes Explained: How They're Already Protecting You and How to Sandbox Any Program, from https://www.howtogeek.com/169139/sandboxes-explained-how-theyre-already-protecting-you-and-how-to-sandbox-any-program/.
1034. What is the sandbox?, from https://chromium.googlesource.com/chromium/src/+/master/docs/design/sandbox_faq.md#What-is-the-sandbox.

1035. JOSH HENDRICKSON, Windows 10's New Sandbox Feature is Everything We've Always Wanted, from https://www.howtogeek.com/399153/windows-10s-new-sandbox-feature-is-everything-weve-always-wanted/.
1036. Lance Whitney, How to Safely Run Software With Windows 10 Sandbox, from https://in.pcmag.com/gallery/131437/how-to-safely-run-software-with-windows-10-sandbox.
1037. Firejail Security Sandbox, from https://firejail.wordpress.com/.
1038. Jay Chen, Making Containers More Isolated: An Overview of Sandboxed Container Technologies, from https://unit42.paloaltonetworks.com/making-containers-more-isolated-an-overview-of-sandboxed-container-technologies/.
1039. Shubham Dubey, Many approaches to sandboxing in Linux, from https://opensourceforu.com/2016/07/many-approaches-sandboxing-linux/.
1040. Shubham Dubey, Sandboxing and program isolation in linux using many approaches (Part 1), from https://nixhacker.com/sandboxing-and-program-isolation-in-linux-using-many-approaches/.
1041. What is a "sandbox"?, from https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/sandboxprotections.html.
1042. Prepare to install Windows Defender Application Guard, from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/install-wd-app-guard.
1043. Application Guard testing scenarios, from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/test-scenarios-wd-app-guard.
1044. Brien Posey, Windows Defender Application Guard: First Look, from https://redmondmag.com/articles/2019/07/11/windows-defender-application-guard.aspx.
1045. Paul Rubens, Patch Management: How to Update Software on Your Network Securely, from https://www.esecurityplanet.com/network-security/patch-management.html.
1046. Patch Management, from https://www.techopedia.com/definition/13835/patch-management.
1047. Paul Rubens, Open Source Patch Management: Options for DIYers, from https://www.esecurityplanet.com/applications/open-source-patch-management.html.
1048. Software Patch Management for Windows Servers and Workstations, from https://www.solarwinds.com/patch-manager/use-cases/software-patch-management-windows.
1049. Rezaduty, Complete Web Application Firewall Guide, from https://medium.com/schkn/web-application-firewall-guide-125645343beb.
1050. Richardh, Benefits of using a Web Application Firewall, Web Application Firewall (WAF), from https://www.rapid7.com/fundamentals/web-application-firewalls/.
1051. Tim Rains, Microsoft's Free Security Tools – URLScan Security Tool, from https://www.microsoft.com/security/blog/2013/01/22/microsofts-free-security-tools-urlscan-security-tool/.
1052. Security Best Practices for the Mobile Enterprise, from https://www.juniper.net/us/en/local/pdf/whitepapers/2000420-en.pdf.
1053. Lance Cleghorn (17 May 2013), Network Defense Methodology, from https://www.scirp.org/pdf/jis_2013071213311297.pdf.
1054. Microsoft Learn. Spark possibility., from https://learn.microsoft.com.
1055. Make better, secure software from the start, from https://www.docker.com.
1056. Firejail Security Sandbox, from https://firejail.wordpress.com/.
1057. What is Cuckoo, from https://cuckoosandbox.org/.
1058. PRODUCT SECURITY ASSESSMENTS, from https://www.deeparmor.com/.

Module 10 Data Security

1059. Futuretech, Data Loss Prevention, from http://www.futuretech-group.com/datalossprevention.html
1060. Wikibooks, Fundamentals of Information Systems Security/Access Control Systems, from https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems
1061. James Martin (August 21, 2019) What is access control? A key component of data security, from https://www.csoonline.com/article/3251714/what-is-access-control-a-key-component-of-data-security.html
1062. NetApp, What Is Backup and Recovery?, from https://www.netapp.com/us/info/what-is-backup-and-recovery.aspx
1063. Blancco (November 2016) The Ultimate Guide to Data Retention, from https://cyber-edge.com/wp-content/uploads/2017/02/Blancco-eBook.pdf
1064. Aseem Kishore (November 13, 2015) How to Set File and Folder Permissions in Windows, from https://www.online-tech-tips.com/computer-tips/set-file-folder-permissions-windows/
1065. SourceDaddy, Configure File System permissions, from https://sourcedaddy.com/windows-10/configure-file-system-permissions.html
1066. Microsoft (May 13, 2019) Enable controlled folder access, from https://docs.microsoft.com/en-in/windows/security/threat-protection/microsoft-defender-atp/enable-controlled-folders
1067. WikiHow (March 29, 2019) How to Prevent Unauthorized Access to Files, from https://www.wikihow.com/Prevent-Unauthorized-Access-to-Files
1068. The Geek Diary, How to Configure ACL (Access Control Lists) in Linux FileSystem, https://www.thegeekdiary.com/how-to-configure-aclaccess-control-lists-in-linux-filesystem/
1069. Kuldeep Sharma (April 22, 2014) Secure Files/Directories using ACLs (Access Control Lists) in Linux, from https://www.tecmint.com/secure-files-using-acls-in-linux/

1070. CloudBT (July 29, 2013) How to configure account lockout policy for a domain on Windows Server, from https://www.it-support.com.au/how-to-configure-account-lockout-policy-on-windows-server/2013/07/
1071. Apple (November 30, 2018) Use FileVault to encrypt the startup disk on your Mac, from https://support.apple.com/en-us/HT204837
1072. UCSF Information Technology, Enable Encryption on Android Devices, from https://it.ucsf.edu/how_do/enable-encryption-android-devices
1073. DuckDuckGo (May 10, 2017) How to Encrypt Your Device, from https://spreadprivacy.com/how-to-encrypt-devices/
1074. Ayush (August 23, 2018) How to encrypt files with EFS Encryption on Windows 10, from https://www.thewindowsclub.com/encrypt-files-efs-encryption-windows-10
1075. Lysa Myers (August 8, 2013) How to Use Apple's Built-in Features to Encrypt Files and Folders, from https://www.intego.com/mac-security-blog/how-to-use-apples-built-in-features-to-encrypt-files-and-folders/
1076. Basit Aalishan Masood-Al-Farooq (July 19, 2012) Using Cell-Level Encryption in SQL Server, from https://www.sqlservercentral.com/blogs/using-cell-level-encryption-in-sql-server
1077. Microsoft (February 1, 2019) Encrypt a Column of Data, from https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/encrypt-a-column-of-data?view=sql-server-ver15
1078. Prashanth Jayaram (October 2, 2017) How to configure Always Encrypted in SQL Server 2016 using SSMS, PowerShell and T-SQL, from https://www.sqlshack.com/configure-always-encrypted-sql-server-2016-using-ssms-powershell-t-sql/
1079. Digicert, IIS 10: Create CSR and Install SSL Certificate, from https://www.digicert.com/csr-creation-ssl-installation-iis-10.htm#ssl_certificate_install
1080. OpenPGP, How PGP Works, from https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html
1081. Eric Geier (April 25, 2012) How to Encrypt Your Email, from https://www.pcworld.com/article/254338/how_to_encrypt_your_email.html
1082. Microsoft, (March 5, 2019) Protect your enterprise data using Windows Information Protection (WIP), from https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/protect-enterprise-data-using-wip
1083. Ed Moyes (July 30, 2019) How to Use Windows Information Protection (WIP) to automatically protect classified files, from http://windowsbulletin.com/how-to-use-windows-information-protection-wip-to-automatically-protect-classified-files/
1084. Susan Ward (October 22, 2015), Data Backup is The Best Data Protection The 3 Steps to Successful Data Backup, from http:// sbinfocanada.about.com/ cs/management/ a/ databackup.htm.
1085. Why back up? The importance of protecting your data , from http://static.highspeedbackbone.net/pdf/hp_why_backup.pdf.
1086. Oct 24, 2010, Choosing backup media is easy when you know how, thanks to this handy guide, from http://www.top-windows-tutorials.com/backup-media/.
1087. Susan Ward (October 22, 2015), Data Backup is The Best Data Protection Which Data Backup Media is Best?, from http:/ /sbinfocanada.about.com /cs /management/a/databackup_2.htm.
1088. Simplifying NAS/SAN Backup and Recovery with Barracuda Backup, from https://www.barracuda.com/assets/docs/White_Papers/Barracuda_Backup_SB_NAS_US.pdf.
1089. Dong Ngo (July 20 216), Synology DiskStation DS1513+, from http://www.cnet.com/topics/storage/best-hard-drives-and-storage/network-attached-storage/.
1090. What is the difference between cold backup and hot backup, from http://www.geekinterview.com/question_details/49691.
1091. Difference between: Full, Differential, and Incremental Backup, from http://www.backup.info/difference-between-full-differential-and-incremental-backup.
1092. Incremental and Differential, from http://www.backup-utility.com/help/incremental-and-differential.html.
1093. System Backup, from http://www.backup-utility.com/help/system-backup.html.
1094. 10 Mar, 2015, What is a Data Backup?, from http://kb.winzip.com/kb/entry/12.
1095. Business Continuity Plan, from http://www.ready.gov/business/implementation/continuity.
1096. IT Disaster Recovery Plan, from http://www.ready.gov/business/implementation/IT.
1097. Kris Bushover,Eric Osterholm (oct 28 2008), Disaster Recovery and Data Backup, from http://www.slideshare.net/spiceworks/disaster-recovery-data-backup-strategies-presentation.
1098. Jaspreet Singh (03.22.08), Understanding RPO and RTO, from http://www.druva.com/blog/understanding-rpo-and-rto/.
1099. ERIC GRIFFITH (MARCH 24, 2016), The Beginner's Guide to PC Backup http://in.pcmag.com/backup-products/75477/feature/the-beginners-guide-to-pc-backup.
1100. Joshua Lockhart (May 30, 2013), Be Prepared: These Are the Vital Files You Should Backup, from http://www.makeuseof.com/tag/be-prepared-these-are-the-vital-files-you-should-backup/.
1101. How Often Do You Need to Back Up Your Files?, from http://www.allbusiness.com/how-often-do-you-need-to-back-up-your-files-1202-1.html.
1102. How Often Should You Backup Your Files?, from http://www.datarecoverylabs.com/how-often-should-you-backup-your-files.html.
1103. 24th Oct 201, Choosing backup media is easy when you know how, thanks to this handy guide DVD/CD Recordable, from http://www.top-windows-tutorials.com/backup-media/#DVDCD.
1104. Selecting the backup medium, from http://www.tldp.org/LDP/sag/html/backup-media.html.
1105. RAID (redundant array of independent disks), from http://searchstorage.techtarget.com/definition/RAID.
1106. Vangie Beal, RAID - redundant array of independent disks, from http://www.webopedia.com/TERM/R/RAID.html.
1107. What is RAID?, from http://www.freeraidrecovery.com/library/what-is-raid.aspx.

1108. Nahar Dijla (SEPTEMBER 1, 2007), Why RAID ? What are the advantages and disadvantages of RAID arrays Servers?, from http://searchwarp.com/swa248158.htm.
1109. Advantages and Disadvantages of RAID, from http://www.hightech-post.com/2011/06/advantages-and-disadvantages-of-raid.html.
1110. RAID controller, from http://searchstorage.techtarget.com/definition/RAID-controller.
1111. Serial ATA (Serial Advanced Technology Attachment or SATA), from http:// searchstorage.techtarget.com/ definition/Serial-ATA.
1112. RAVI PRAKASH AND SHIVENDRA SINGH, Improving RAID Storage Systems with Non-volatile Write Journals, from http://www.osslab.org.tw/Storage/Enterprise/SAS%E8%88%87RAID/RAID_Technology_Articles/Improving_RAID_Storage_Systems_with_Non-volatile_Write_Journals.
1113. Disk array controller, from https://en.wikipedia.org/wiki/Disk_array_controller.
1114. SCSI Vs. SATA Vs. IDE, from http://www.buzzle.com/articles/scsi-vs-sata-vs-ide.html.
1115. RAID, from http://www.prepressure.com/library/technology/raid.
1116. RAID 30 And RAID 50 , from http://www.powerdatarecovery.com/data-recovery/raid30-and-raid50.html.
1117. Antony Adshead (14 Sep 2009), Software RAID vs hardware RAID: Pros and cons , from http://www.computerweekly.com/news/1367590/Software-RAID-vs-hardware-RAID-Pros-and-cons.
1118. Hardware RAID versus Software RAID , from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/System_Administration_Guide/s1-raid-approaches.html.
1119. Logan Hibbitt , MCIPT Guide to Microsoft Windows Server 2008 Server Administration (Exam # 70 -646) Configuring and Managing Data Storage, from http://slideplayer.com/slide/1517307/.
1120. Brien Posey, Best practices for setting up RAID groups, from http://searchdatacenter.techtarget.com/tip/Best-practices-for-setting-up-RAID-groups.
1121. Scott Lawe (Oct 10, 2010), Choose a RAID level that works for you, from http://www.techrepublic.com/blog/the-enterprise-cloud/choose-a-raid-level-that-works-for-you/.
1122. Storage area network , from https://en.wikipedia.org/wiki/Storage_area_network.
1123. Ericka Headley, D–Link Specified Specialist Storage, from http://slideplayer.com/slide/3388022/.
1124. Storage Area Network (SAN), from http://www.slideserve.com/ula/storage-area-network-san.
1125. Sarath Pillai (04/19/2014), SAN vs NAS - Difference between a Storage Area Network and Network Attached Storage http://www.slashroot.in/san-vs-nas-difference-between-storage-area-network-and-network-attached-storage.
1126. Difference between SAN and NAS architecture, from http://searchstorage.techtarget.com/answer/The-difference-between-SAN-and-NAS.
1127. CODY PIERSON, WHAT ARE THE ADVANTAGES OF A STORAGE AREA NETWORK (SAN)?, from http://www.prophet.ca/what-are-the-advantages-of-a-storage-area-network-san/.
1128. Christopher Poelker, The benefits of SAN attached storage, from http://searchstorage.techtarget.com/answer/The-benefits-of-SAN-attached-storage.
1129. Lynn Boone, Introduction to Network and Networking Concepts, from http://slideplayer.com/slide/7076497/.
1130. Junaid Aziz Khokhar, Storage Area Network, from http://www.slideshare.net/masterubaid/storage-area-network-25251039.
1131. Raphael Ejike, Stroage Area Network (SAN) , from http://pt.slideshare.net/raphaelejike/storage-area-network-san-4892728.
1132. Storage Area Network Architecture (SAN Architecture) , from https://www.techopedia.com/definition/30211/storage-area-network-architecture-san-architecture.
1133. Keith Spayth (May 14, 1010), Storage Area Network, from http://www.slideshare.net/itsec/san-review.
1134. Network-attached storage, from https://en.wikipedia.org/wiki/Network-attached_storage.
1135. Vangie Beal, NAS - Network Attached Storage http://www.webopedia.com/TERM/N/network-attached_storage.html.
1136. network-attached storage (NAS) , from http://searchstorage.techtarget.com/definition/network-attached-storage.
1137. Network Attached Storage (NAS) Review: Pros and Cons, from http://www.bffnas.com/network-attached-storage-nas-overview-on-its-pros-and-cons/.
1138. Rajesh K (Oct 29, 2010), NAS – Advantages, Limitations & Recommendations for Ethernet Storage over TCP/IP Networks, from http://www.excitingip.com/819/network-attached-storage-advantages-limitations-ethernet-storage-ip-network-best-practices/.
1139. Sandeep Gopalreddy,Network Attached Storage (NAS), from http://www.slideshare.net/sandeepgodfather/network-attached-storage-nas.
1140. NAS/ SAN, from http://www.powershow.com/view/2e88a-YWY2O/NAS_SAN_powerpoint_ppt_presentation.
1141. What Are the Difference between NAS and File Server?, from http://www.bffnas.com/what-are-the-difference-between-nas-and-file-server/.
1142. Walter Glenn (01/8/13), Do You Run a Home Server or NAS?, from http://lifehacker.com/5974253/do-you-run-a-home-server-or-nas.
1143. Burleson, Oracle Concepts - Backup and Recovery Concepts, from http://www.dba-oracle.com/concepts/backup_recovery.htm.
1144. Ethical Hacking & Info Security Training Program, Database Security, from http://www.tutorialized.com/tutorial/Database-Backups-Hot-Backup-vs.-Cold-Backup/27348.
1145. cold backup (offline backup), from http://searchstorage.techtarget.com/definition/cold-backup.
1146. hot backup (dynamic backup), from http://searchstorage.techtarget.com/definition/hot-backup.
1147. Vangie Beal, structured data, from http://www.webopedia.com/TERM/S/structured_data.html.
1148. Brien Posey, Data backup types explained: Full, incremental, differential and incremental-forever backup, from http://searchdatabackup.techtarget.com/tip/Data-backup-types-explained-Full-incremental-differential-and-incremental-forever-backup.

1149. Types of backup (January 21, 2005), https://technet.microsoft.com/en-us/library/cc784306(v=ws.10).aspx.
1150. Backup Solutions from Third Parties, from http://support.postbox-inc.com/hc/en-us/articles/202200050-Backup-Solutions-from-Third-Parties.
1151. Jasson Buffington (January 2015), A checklist when choosing a backup solution for SaaS based Applications http://cdn2.hubspot.net/hubfs/441981/ESG_Cloud_BackUP_Asigra_Jan_2015.pdf?t=1442236384300.
1152. September 12, 2014, Why You should be using Third Party Backup Services, from http://www.volico.com/why-you-should-be-using-third-party-backup-services/.
1153. Symantec Storage Foundation Basic , from https://www.veritas.com/content/veritas/english/en/search.html?q=symantec%20storage%20foundation%20&gsaSearchJson={%22filter%22:[],%22startPage%22:1,%22start%22:0,%22sort%22:%22date:D:L:d1%22}.
1154. Cisco Prime Data Center Network Manager , from http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-data-center-network-manager/index.html.
1155. Eric Geier, How to Encrypt Your Email, from HYPERLINK "https://www.pcworld.com/article/254338/how_to_encrypt_your_email.html"https://www.pcworld.com/article/254338/how_to_encrypt_your_email.html. HYPERLINK "https://www.pcworld.com/article/254338/how_to_encrypt_your_email.html"
1156. Laura Spence, MS Outlook: How to Secure Your Account & Encrypt Emails, from https://business.tutsplus.com/tutorials/outlook-how-to-encrypt-emails--cms-31516.
1157. Encryption 101: How to Enable Email Encryption on Outlook, from https://www.trendmicro.com/vinfo/pl/security/news/online-privacy/encryption-101-how-to-enable-email-encryption-on-outlook.
1158. Encrypt email messages, from https://support.office.com/en-us/article/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc.
1159. Arianna Etemadieh, How to Encrypt Your Gmail Email, from https://www.paubox.com/blog/gmail-encryption-settings.
1160. JR Raphael, Gmail encryption: Everything you need to know, from https://www.computerworld.com/article/3322497/gmail-encryption.html.
1161. Cheryl Tang
1162. Reasons to Include Data Masking in Your Data Security Strategy, from https://www.imperva.com/blog/top-3-reasons-include-data-masking-data-security-strategy/.
1163. Keith Bromley, Data Masking: The ABCs of Network Visibility, from https://www.ixiacom.com/company/blog/data-masking-abcs-network-visibility.
1164. Stephen Watts, What is Data Masking? Data Masking Explained, from https://www.bmc.com/blogs/data-masking/.
1165. Ben Campbell, Why Data Masking Needs to Be in Every Data Security Strategy, from https://www.tripwire.com/state-of-security/security-data-protection/eyes-data-masking-needs-every-data-security-strategy/.
1166. Steve Pomroy, Static Versus Dynamic Data Masking, from https://www.imperva.com/blog/static-versus-dynamic-data-masking/.
1167. CHESKY RON, What is Data Masking?, from https://www.techwalls.com/data-masking-explained/.
1168. Data masking, from https://en.wikipedia.org/wiki/Data_masking#Different_types.
1169. What is Data Obfuscation?, from https://www.talend.com/resources/data-obfuscation/.
1170. Kashif-Sohail, Dynamic Data Masking, from https://www.codeproject.com/Articles/1084808/Dynamic-Data-Masking-in-SQL-Server.
1171. Dynamic Data Masking, from https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-2017.
1172. Pankaj Chakole, Dynamic Data Masking Feature in SQL Server 2016, from https://www.sqlservercentral.com/articles/dynamic-data-masking-feature-in-sql-server-2016.
1173. Naveen Sharma, How To Implement SQL Server Dynamic Data Masking?, from https://www.sqlmvp.org/implement-dynamic-data-masking/.
1174. Implementing Data Masking, from http://www.oracle.com/us/products/database/data-masking-best-practices-161213.pdf.
1175. Oracle Data Masking and Subsetting Pack, from https://www.oracle.com.
1176. Ian Paul, How to use Windows 10's File History backup feature, from https://www.pcworld.com/article/2974385/how-to-use-windows-10s-file-history-backup-feature.html.
1177. Back up and restore your PC, from https://support.microsoft.com/en-in/help/17127/windows-back-up-restore.
1178. Backup and Restore in Windows 10, from https://support.microsoft.com/en-in/help/4027408/windows-10-backup-and-restore.
1179. Derrik Diener, Back Up Your Entire Hard Drive on Linux using Gnome Disk Utility, from https://www.maketecheasier.com/back-up-entire-hard-drive-linux/.
1180. BRYAN M WOLFE, How to selectively back up with Time Machine, from https://www.imore.com/how-selectively-back-time-machine.
1181. Jack Wallen, Total System Backup And Recall With Déjà Dup, from https://www.linux.com/tutorials/total-system-backup-and-recall-deja-dup/.
1182. Create a Full Database Backup, from https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server?view=sql-server-ver15.
1183. MS SQL Server - Creating Backups, from https://www.tutorialspoint.com/ms_sql_server/ms_sql_server_creating_backups.htm.
1184. Back Up and Restore of SQL Server Databases, from https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/back-up-and-restore-of-sql-server-databases?view=sql-server-ver15.
1185. Whole Database Backup, from https://docs.oracle.com/database/121/ADMQS/GUID-E6AB87FC-DE6E-433C-AB61-F2055B6CC547.htm.
1186. Back up your email, from https://support.office.com/en-us/article/back-up-your-email-e5845b0b-1aeb-424f-924c-aa1c33b18833.

1187. Backup and Restore all Outlook data, from https://www.howto-outlook.com/howto/backupandrestore.htm.
1188. Michael Crider, export and import your Outlook inbox, from https://www.digitaltrends.com/computing/how-to-backup-emails-calendars-and-contacts-in-microsoft-outlook/.
1189. Email Backup in GmailGoogle Takeout, from https://takeout.google.com/?hl=en&pli=1.
1190. Backup and Restore IIS configuration to Another Server, from http://woshub.com/how-to-backup-and-restore-iis-configuration-to-another-server/.
1191. Chris Lazari, Backup and Restore IIS on Windows Server 2016, from https://chrislazari.com/backup-and-restore-iis-on-windows-server-2016/.
1192. Brad Litwin, Backup Your Website, from https://www.a2hosting.com/blog/need-backup-website/.
1193. Generate & Download a Website Backup, from https://www.hostgator.com/help/article/how-to-generatedownload-a-full-backup.
1194. Margaret Rouse, data retention policy, from https://searchdatabackup.techtarget.com/definition/data-retention-policy.
1195. Mark Keppler, Steps to Developing a Solid Data Retention Policy, from https://www.ispartnersllc.com/blog/5-steps-developing-data-retention-policy/.
1196. Data Retention Policy, from https://www.5nine.com/data-retention-policy/.
1197. Margaret Rouse, data retention, from https://searchstorage.techtarget.com/definition/data-retention.
1198. Mauro Huculak (02 Jan 2023), How to enable TPM and Secure Boot in BIOS for Windows 11, from https://pureinfotech.com/check-enable-tpm-secure-boot-install-windows-11/#google_vignette%E2%80%8B.
1199. How to enable TPM, from https://support.microsoft.com/en-us/windows/enable-tpm-2-0-on-your-pc-1fd5a332-360d-4f46-a1e7-ae6b0c90645c#bkmk_enable_tpm.
1200. Data at Rest, from https://www.imperva.com/learn/data-security/data-at-rest/.
1201. Sabrina Lupșan (09 Aug 2022), Types of Encryption for in Motion, in Use, at Rest Data, from https://cyscale.com/blog/types-of-encryption/.
1202. Christopher Tozzi (17 Nov 2022), The Quick Guide to Data Encryption Best Practices, from https://www.precisely.com/blog/data-security/data-encryption-101-guide-best-practices.
1203. What is a Data Federation, from https://www.tibco.com/reference-center/what-is-a-data-federation#:~:text=A%20data%20federation%20is%20a,data%20for%20front%2Dend%20applications.
1204. Advanced Encryption Standard, from https://www.geeksforgeeks.org/advanced-encryption-standard-aes/.
1205. What is data integrity and why is it important, from https://www.talend.com/resources/what-is-data-integrity/.
1206. Catherine Cote (04 Feb 2021), WHAT IS DATA INTEGRITY AND WHY DOES IT MATTER, from https://online.hbs.edu/blog/post/what-is-data-integrity.
1207. Chris Brook (08 May 2023), What is Data Integrity, from https://www.digitalguardian.com/blog/what-data-integrity-data-protection-101.
1208. Jonathan Johnson (15 Feb 2022), Data Integrity vs Data Quality: An Introduction, from https://www.bmc.com/blogs/data-integrity-vs-data-quality/.
1209. Stepen Bigelow, Data Integrity, from https://www.techtarget.com/searchdatacenter/definition/integrity.
1210. Anthony Corbo (03 Jan 2023), What Is Data Integrity, from https://builtin.com/data-science/data-integrity.
1211. What is data integrity, from https://www.javatpoint.com/what-is-data-integrity.
1212. Data Integrity, from https://csrc.nist.gov/glossary/term/data_integrity.
1213. 29 Nov 2023, What Is Data Integrity, from https://www.coursera.org/articles/what-is-data-integrity.
1214. What Is Data Integrity, from https://www.fortinet.com/resources/cyberglossary/data-integrity#:~:text=Data%20integrity%20is%20a%20concept,correct%20data%20in%20their%20database.
1215. 14 Nov 2022, Data Integrity vs. Data Quality, from https://www.precisely.com/blog/data-integrity/data-integrity-vs-data-quality-different.
1216. Nimrod (26 Oct 2022), Data Quality vs Data Integrity, from https://www.polar.security/post/data-quality-vs-data-integrity.

Module 11 Enterprise Virtual Network Security

1217. Marlese Lessing (September 2019) Understanding the SDN Architecture - SDN Control Plane & SDN Data Plane, from https://www.sdxcentral.com/networking/sdn/definitions/inside-sdn-architecture/.
1218. Connor Craven (January 2020) What is Software Defined Networking (SDN)? Definition, from https://www.sdxcentral.com/networking/sdn/definitions/what-the-definition-of-software-defined-networking-sdn/.
1219. Blueplanet, What is SDN?, from https://www.blueplanet.com/resources/What-is-SDN.html.
1220. Kristian Slavov, Daniel Migault, and Makan Pourzandi (August 31, 2015) Identifying and Addressing the Vulnerabilities and Security Issues of SDN, from https://www.ericsson.com/4ae131/assets/local/reports-papers/ericsson-technology-review/docs/2015/etr-sdn-security.pdf.
1221. SDxCentral Staff (April 27, 2016) What Is NFV Infrastructure (NFVI)? Definition, from https://www.sdxcentral.com/networking/nfv/definitions/nfv-infrastructure-nfvi-definition/.
1222. Techplayon (August 8, 2017) Network Function Virtualization (NFV) Architecture, from http://www.techplayon.com/network-function-virtualization-nfv-architecture/.
1223. IpCisco, NFV Infrastructure, from https://ipcisco.com/lesson/nfv-infrastructure/.
1224. Akamai, Cloud Networking, from https://www.akamai.com/us/en/resources/cloud-network.jsp.
1225. Eugene (August 7, 2017) Virtualization Techniques in Cloud Computing, from https://www.sam-solutions.com/blog/virtualization-techniques-in-cloud-computing/.

1226. Namrata Bisht, Virtualization in Cloud Computing and Types, from https://www.geeksforgeeks.org/virtualization-cloud-computing-types/.
1227. Shaikh Abdul Azeem, Satyendra Kumar Sharma (September 2017) Role of Network Virtualization in Cloud Computing and Network Convergence, from http://www.iraj.in/journal/journal_file/journal_pdf/3-400-1512365019136-140.pdf.
1228. eTutorials, VLAN-Based Network Attacks, from http://etutorials.org/Networking/lan+switching/Chapter+9.+Switching+Security/VLAN-Based+Network+Attacks/.
1229. Rene Molenaar, VLAN Hopping, from https://networklessons.com/cisco/ccnp-switch/vlan-hopping.
1230. Cisco Network Academy, VLAN Security and Design, from https://static-course-assets.s3.amazonaws.com/RSE50ENU/module3/3.3.1.1/3.3.1.1.html.
1231. CSIT, Secure Communications Network, from https://coinsrs.no/wp-content/uploads/2018/08/metochi2018-scotthayward-COINS2018_SDNSec_SSH_Slides-2.pdf.
1232. Arash Shaghaghi, Mohamed Ali Kaafar, Rajkumar Buyya, Sanjay Jha (April 1, 2018) Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions, from https://arxiv.org/pdf/1804.00262.pdf.
1233. Gabor Nagy (May 19, 2015) Operating System Containers vs. Application Containers, from https://blog.risingstack.com/operating-system-containers-vs-application-containers/.
1234. Murugiah Souppaya, John Morello, Karen Scarfone Application Container Security Guide (September 2017) from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf.
1235. Aqua, Docker Architecture, from https://wiki.aquasec.com/display/containers/Docker+Architecture.
1236. Mark Church, Marlon Ruiz, Andrew Seifert, Trapier Marshall, Docker Swarm Reference Architecture: Exploring Scalable, Portable Docker Container Networks, from https://success.docker.com/article/networking.
1237. Khaja Ibrahim (October 5, 2019) Docker Networking Series – I, from https://directdevops.blog/2019/10/05/docker-networking-series-i/.
1238. Kubernetes (January 16, 2020) Kubernetes Components, from https://kubernetes.io/docs/concepts/overview/components/.
1239. Prasad Katti, Kubernetes Design and Architecture, from https://github.com/kubernetes/community/blob/master/contributors/design-proposals/architecture/architecture.md#the-kubernetes-node.
1240. Kubernetes, Production-Grade Container Orchestration, from https://kubernetes.io/'
1241. Amir Jerbi (January 5, 2017) 8 Docker security rules to live by, from https://www.infoworld.com/article/3154711/8-docker-security-rules-to-live-by.html.
1242. Aria (September 27, 2018) Security Challenges Related to Containers, from https://www.ariacybersecurity.com/container-security-challenges-blog/.
1243. Christopher Tozzi (August 6, 2018) 3 Container Security Advantages and 3 Security Challenges, from https://containerjournal.com/topics/container-security/3-container-security-advantages-and-3-security-challenges/.
1244. Trend Micro (May 14, 2019) Container Security: Examining Potential Threats to the Container Environment, from https://www.trendmicro.com/vinfo/us/security/news/security-technology/container-security-examining-potential-threats-to-the-container-environment.
1245. Shira Caldie (September 22, 2017) Using Docker containers? Beware of these security risks, from https://www.ontrack.com/uk/blog/the-world-of-data/using-docker-containers-beware-of-these-security-risks/.
1246. Chuck Hegarty (August 31, 2018) Understanding Container Security, from https://www.siriuscom.com/2018/08/understanding-container-security/.
1247. Patrick Kleindienst (August 16, 2016) Exploring Docker Security – Part 2: Container flaws, from https://blog.mi.hdm-stuttgart.de/index.php/2016/08/16/exploring-docker-security-part-2-container-flaws/.
1248. Infosec (June 21, 2012) Virtualization Security in Cloud Computing, from https://resources.infosecinstitute.com/virtualization-security-cloud-computing/#gref.
1249. Microsoft Azure (September 17, 2018) Time sync for Windows VMs in Azure, from https://docs.microsoft.com/en-us/azure/virtual-machines/windows/time-sync.
1250. Margaret Rouse (October 2017) Windows 10 Isolated User Mode (IUM), from https://searchenterprisedesktop.techtarget.com/definition/Windows-10-Isolated-User-Mode-IUM.
1251. Microsoft (August 31, 2016) Deploy Hyper-V over SMB, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj134187(v%3Dws.11).
1252. OmniSecu, How to prevent MAC flooding attacks by configuring switchport port-security, from https://www.omnisecu.com/ccna-security/how-to-prevent-mac-flooding-attacks-by-configuring-switchport-port-security.php.
1253. Cisco, Cisco MDS 9000 Family NX-OS Security Configuration Guide, from https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_0/configuration/guides/sec/nxos/sec.html.
1254. Cisco, Wired 802.1X Deployment Guide, from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html.
1255. Cisco, Routing and Bridging Guide vA1(7), Cisco ACE 4700 Series Application Control Engine Appliance, from https://www.cisco.com/c/en/us/td/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/routing_bridging/guide/rtbrgdgd/arp.html.
1256. Valter Popeskic, Mitigate VLAN hopping attack – Get rid of Layer 2 attacks, from https://howdoesinternetwork.com/2012/mitigate-vlan-hopping.
1257. Eric Leahy (July 5, 2011) BPDU Guard, BPDU Filter, Root Guard, Loop Guard & UDLD, from http://ericleahy.com/index.php/bpdu-guard-bpdu-filter-root-guard-loop-guard-udld/.

1258. Montida Pattaranantakul, Ruan He, Ahmed Meddahi, Zonghua Zhang (August 2016) SecMANO: Towards Network Functions Virtualization (NFV) Based Security MANagement and Orchestration, from https://www.researchgate.net/publication/316212661_SecMANO_Towards_Network_Functions_Virtualization_NFV_Based_Security_MANagement_and_Orchestration.

1259. Shankar Lal, Tarik Taleb, Ashutosh Dutta (2017) NFV: Security Threats and Best Practices, from http://anastacia-h2020.eu/publications/NFV_Security_Threats_and_Best_Practices.pdf.

1260. NeuVector, Network Security, from https://neuvector.com/container-network-security-solutions/.

1261. Rani Osnat (December 3, 2018) Top Docker Security Best Practices, from https://blog.aquasec.com/docker-security-best-practices.

1262. David Bisson (October 11, 2018) Clarifying the Misconceptions: Monitoring and Auditing for Container Security, from https://www.tripwire.com/state-of-security/devops/clarifying-the-misconceptions-monitoring-and-auditing-for-container-security/.

1263. Docker docs, Docker Security, from https://docs.docker.com/engine/security/security/.

1264. Red Hat, Chapter 3. Signing Container Images, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux_atomic_host/7/html/managing_containers/signing_container_images.

1265. Docker docs, Seccomp security profiles for Docker, from https://docs.docker.com/engine/security/seccomp/.

1266. Philipp Schmied (March 27, 2019) Linux Container Basics: Capabilities, from https://www.schutzwerk.com/en/43/posts/linux_container_capabilities/.

1267. Docker docs, Isolate containers with a user namespace, from https://docs.docker.com/engine/security/userns-remap/.

1268. Docker docs, Content trust in Docker, from https://docs.docker.com/engine/security/trust/content_trust/#image-tags-and-content-trust.

1269. Docker docs, Runtime options with Memory, CPUs, and GPUs, from https://docs.docker.com/config/containers.

1270. Jack Wallen (April 10, 2017) 5 tips for securing your Docker containers, from https://www.techrepublic.com/article/5-tips-for-securing-your-docker-containers/.

1271. Synk, Docker Image Security Best Practices, from https://res.cloudinary.com/snyk/image/upload/v1551798390/Docker_Image_Security_Best_Practices_.pdf.

1272. Margaret Rouse, virtualization, from https://searchservervirtualization.techtarget.com/definition/virtualization.

1273. What is virtualization?, from https://www.citrix.com/en-in/glossary/what-is-virtualization.html.

1274. Virtualization, from https://www.techopedia.com/definition/719/virtualization.

1275. What is Virtualization, from https://www.igi-global.com/dictionary/an-evolutionary-approach-for-load-balancing-in-cloud-computing/31852.

1276. What is virtualisation?, from https://www.itpro.co.uk/612016/what-is-virtualisation.

1277. Virtualisation | Server Virtualisation, from http://www.artofcomputing.com/virtualisation-virtual-servers.html.

1278. Vikas Garg, VIRTUALIZATION, from http://www.ijoart.org/papers/VIRTUALIZATION.html.

1279. Physical and virtual architecture, from https://subscription.packtpub.com/book/virtualization_and_cloud/9781782174851/1/ch01lvl1sec08/physical-and-virtual-architecture.

1280. What is Network Virtualization (NV)?, from https://www.vmware.com/topics/glossary/content/network-virtualization.

1281. Network virtualization explained, from https://searchitchannel.techtarget.com/feature/Network-virtualization-explained.

1282. Network Virtualization and Virtual Networks, from https://docs.oracle.com/cd/E19120-01/open.solaris/819-6990/gfkbw/index.html.

1283. Using a Virtual Network With Logical Domains, from https://docs.oracle.com/cd/E19053-01/ldoms.mgr11/820-4913-10/chapter7.html.

1284. Network Virtualization, from https://www.techopedia.com/definition/655/network-virtualization.

1285. Network Virtualization, from https://networksandservers.blogspot.com/2011/10/virtualization-ii.html.

1286. Overview of Network Virtualization, from https://docs.oracle.com/cd/E26502_01/html/E28992/gfkbw.html.

1287. N.M. Mosharaf Kabir Chowdhury, Raouf Boutaba, A survey of network virtualization, from http://www.mmc.geofisica.unam.mx/acl/MV/CursoMaquinasVirtuales/VirtualizacionEnLinuxCon-RedyDatos/A%20survey%20of%20network%20virtualization.pdf.

1288. VMware Virtual Networking Concepts, from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/virtual_networking_concepts.pdf.

1289. Create and Manage Virtual Networks, from http://www.vce-download.net/study-guide/vmware-vcp-3.10-create-and-manage-virtual-networks.html.

1290. What is Internal Network Virtualization and External Network Virtualization, from http://virtualizationtutor.com/what-is-internal-network-virtualization-and-external-network-virtualization/.

1291. Layer 3 intelligent/managed switches vendors – CISCO, from https://www.moxa.com.

1292. VLAN Trunk Cisco IOS, from https://mars.merhot.dk/w/index.php/VLAN_Trunk_Cisco_IOS.

1293. How to verify and configure VLANs & trunking, from https://www.examcollection.com/certification-training/ccnp-configure-and-verify-vlans-and-trunking.html.

1294. Container security, from https://www.redhat.com/en/topics/security/container-security.

1295. Muhammad Kazim, Rahat Masood, Muhammad Shibli, Abdul Abbasi, Security Aspects of Virtualization in Cloud Computing, from https://hal.inria.fr/hal-01496070/document.

1296. Mark Dargin, NETWORK DESIGN SPOTLIGHT, from https://www.networkworld.com/article/3245173/secure-your-sdn-controller.html.

1297. Scott Hogg, CORE NETWORKING, from https://www.networkworld.com/article/2840273/sdn-security-attack-vectors-and-sdn-hardening.html.

1298. JunHuy Lam , Sang-Gon Lee , Hoon-Jae Lee, and Yustus Eko Oktian, Securing SDN Southbound and Data Plane Communication with IBC, from https://www.hindawi.com/journals/misy/2016/1708970/.

1299. ZHANG Yunyong, XU Lei, and TAO Ye, SDN Based Security Services, from https://res-www.zte.com.cn/mediares/magazine/publication/com_en/article/201804/ZHANGYunyong.pdf.

1300. Adnan Akhunzada, Muhammad Ali Imran, Abdullah Gani, Securing the Software Defined Networks: Taxonomy, Requirements, and Open Issues, from https://www.researchgate.net/publication/271269770_Securing_the_Software_Defined_Networks_Taxonomy_Requirements_and_Open_Issues.

1301. Anatomy of Container Attack Vectors and Mitigations, from https://www.bankinfosecurity.com/anatomy-container-attack-vectors-mitigations-a-12490.

1302. A sleeping security threat: How to protect against container compromise, from https://www.scmagazine.com/home/opinion/executive-insight/a-sleeping-security-threat-how-to-protect-against-container-compromise/.

1303. Robail Yasrab, Mitigating Docker Security Issues, from https://arxiv.org/ftp/arxiv/papers/1804/1804.05039.pdf.

1304. Murugiah Souppaya, John Morello, Karen Scarfone, Application Container Security Guide, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf.

1305. Steven Vaughan-Nichols, Ways to secure your containers, from https://www.hpe.com/us/en/insights/articles/5-ways-to-secure-your-containers-1904.html.

1306. Devdatta Mulgund, Best Practices for Application Container Security, from https://securityintelligence.com/posts/8-best-practices-for-application-container-security/.

1307. What is Software-Defined Security?, from https://www.sdxcentral.com/security/definitions/what-is-software-defined-security/.

1308. Enabling Technologies towards Next Generation Mobile Systems and Networks, from https://www.hindawi.com/journals/misy/2016/1708970/.

1309. Arash Shaghaghi, Mohamed Ali Kaafar, Rajkumar Buyya, Sanjay Jha, Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions, from https://arxiv.org/pdf/1804.00262.pdf.

1310. Adnan Akhunzada, Nor Badrul Anuar, Abdullah Gani, Ahmad khoirul Aziz, Secure and Dependable Software Defined Networks, from https://www.researchgate.net/publication/285781811_Secure_and_Dependable_Software_Defined_Networs.

1311. Jeff, Container Security with Phil Estes, from https://softwareengineeringdaily.com/2016/09/26/container-security-with-phil-estes/.

1312. What is NFV (Network Functions Virtualization)? Definition, from https://www.sdxcentral.com/networking/nfv/definitions/whats-network-functions-virtualization-nfv/.

1313. Lee Doyle, What is NFV and what are its benefits, from https://www.networkworld.com/article/3253118/what-is-nfv-and-what-are-its-benefits.html.

1314. Gokhan Kosem, NFV Infrastructure, from https://ipcisco.com/lesson/nfv-infrastructure/.

1315. Network Functions Virtualisation (NFV): Architectural Framework, from https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf.

1316. What is Network Functions Virtualization?, from https://www.juniper.net/us/en/products-services/what-is/network-functions-virtualization/.

1317. What is NFV?, from https://www.redhat.com/en/topics/virtualization/what-is-nfv.

1318. What is NFV?, from https://www.ciena.com/insights/what-is/What-is-Network-Functions-Virtualization.html.

1319. Bo Gowan, What is Network Function Virtualization (NFV)?, from https://www.ciena.com/insights/articles/What-is-NFV-prx.html.

1320. Francois Reynaud, Francois-Xavier Aguessy, Olivier Bettan, Mathieu Bouet, Attacks against Network Functions Virtualization and Software-Defined Networking: State-of-the-art, from https://www.researchgate.net/publication/304816471_Attacks_against_Network_Functions_Virtualization_and_Software-Defined_Networking_State-of-the-art.

1321. Khushboo Nigam, SECURITY IN NETWORK FUNCTION VIRTUALIZATION, from https://www.linkedin.com/pulse/security-network-function-virtualization-khushboo-nigam.

1322. Montida Pattaranantakul, Ruan He, Ahmed Meddahi, Zonghua Zhang, SecMANO: Towards Network Functions Virtualization (NFV) Based Security MANagement and Orchestration, from https://www.researchgate.net/publication/316212661_SecMANO_Towards_Network_Functions_Virtualization_NFV_Based_Security_MANagement_and_Orchestration.

1323. Doug Hyde, A Survey on the Security of Virtual Machines, from https://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/#sec4.

1324. Ahmed M Alwakeel, Abdulrahman Alnaim, Eduardo B. Fernández, A Survey of Network Function Virtualization Security, from https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security.

1325. Shankar Lal, Tarik Taleb, and Ashutosh Dutta, NFV: Security Threats and Best Practices, from http://anastacia-h2020.eu/publications/NFV_Security_Threats_and_Best_Practices.pdf.

1326. Chandani Vaya, A journey to Kubernetes security, from https://developer.ibm.com/technologies/containers/articles/journey-to-kubernetes-security/.

1327. Connor Gilbert, 9 Kubernetes Security Best Practices Everyone Must Follow, from https://www.cncf.io/blog/2019/01/14/9-kubernetes-security-best-practices-everyone-must-follow/.

1328. Chris Cooney, Security as Standard in the Land of Kubernetes, from https://www.freecodecamp.org/news/security-as-standard-in-the-land-of-kubernetes-50bfad74ca16/.

1329. 15 Kubernetes security best practice to secure your cluster, from https://www.mobilise.cloud/15-kubernetes-security-best-practice-to-secure-your-cluster/.
1330. 11 Ways (Not) to Get Hacked, from https://kubernetes.io/blog/2018/07/18/11-ways-not-to-get-hacked/.
1331. Ajmal Kohgadai, Docker Container Security 101: Risks and 33 Best Practices, from https://www.stackrox.com/post/2019/09/docker-security-101/.
1332. Best practices for building containers, from https://cloud.google.com/solutions/best-practices-for-building-containers.
1333. Docker Images, from https://www.katacoda.com/courses/docker/2.
1334. Andrew Martin, Enable RBAC with Least Privilege, Disable ABAC, and Monitor Logs, from https://kubernetes.io/blog/2018/07/18/11-ways-not-to-get-hacked/#2-enable-rbac-with-least-privilege-disable-abac-and-monitor-logs.
1335. isha Girdhar, RBAC in Kubernetes: Demystified, from https://medium.com/@ishagirdhar/rbac-in-kubernetes-demystified-72424901fcb3.
1336. Daniel Chernenkov, What is RBAC in Kubernetes?, from https://medium.com/@danielckv/what-is-rbac-in-kubernetes-c54457eff2dc.
1337. Eviatar Gerzi, Securing Kubernetes Clusters by Eliminating Risky Permissions, from https://www.cyberark.com/threat-research-blog/securing-kubernetes-clusters-by-eliminating-risky-permissions/.
1338. Using RBAC Authorization, from https://kubernetes.io/docs/reference/access-authn-authz/rbac/.
1339. Securing a Cluster, from https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/#use-transport-level-security-tls-for-all-api-traffic.
1340. Kubernetes Components, from https://kubernetes.io/docs/concepts/overview/components/#control-plane-components.
1341. Auditing, from https://kubernetes.io/docs/tasks/debug-application-cluster/audit/.
1342. Network Policies, from https://kubernetes.io/docs/concepts/services-networking/network-policies/.
1343. Declare Network Policy, from https://kubernetes.io/docs/tasks/administer-cluster/declare-network-policy/.
1344. Secure A Kubernetes Cluster With Pod Security Policies, from https://docs.bitnami.com/kubernetes/how-to/secure-kubernetes-cluster-psp/.
1345. Encrypting Secret Data at Rest, from https://kubernetes.io/docs/tasks/administer-cluster/encrypt-data/.
1346. Secrets, from https://kubernetes.io/docs/concepts/configuration/secret/#using-secrets.
1347. Kubernetes CIS Benchmark, from www.cisecurity.org.
1348. Suraj Kale (14 Jan 2023), Run multiple process on docker container in simple words, from https://medium.com/@kales5078/run-multiple-process-on-docker-container-24fdb170532c.
1349. How do you keep operating system containers up-to-date in production, from https://www.linkedin.com/advice/3/how-do-you-keep-operating-system-containers-up-to-date.
1350. Container Security for developers, from https://snyk.io/learn/container-security/.
1351. Deepti Dilip Jobanputra (20 Oct 2020), Container Platform and Security, from https://www.ashnik.com/back-to-basics-container-technology-security-and-monitoring/.
1352. Rapid 7 (15 Sep 2015), Log Analysis for Containers, from https://www.rapid7.com/blog/post/2015/09/15/log-analysis-for-containers/.
1353. Container Runtime Policies, from https://qualysguard.qg2.apps.qualys.com/cs/help/crs/policies.htm.
1354. What Is Container Security, from https://www.trendmicro.com/en_in/what-is/container-security.html.
1355. Application-Level Scanning: SCA, SAST, DAST, from https://www.aquasec.com/cloud-native-academy/container-security/container-security/#:~:text=Application%2DLevel%20Scanning%3A%20SCA%2C%20SAST%2C%20DAST&text=These%20could%20be%20open%2Dsource,vulnerabilities%20if%20not%20properly%20managed.
1356. Ramkrushna Maheshwar (28 Jul 2023), Best Practices for Secure Docker Containerization, from https://medium.com/@maheshwar.ramkrushna/best-practices-for-secure-docker-containerization-non-root-user-read-only-volumes-and-resource-d34ed09b1bd3.
1357. 14 Feb 2018, Secure the container platform by building a chain of trust, from https://hostingjournalist.com/secure-the-container-platform-by-building-a-chain-of-trust/.
1358. Ensure a separate partition for containers has been created, from https://www.tenable.com/audits/items/CIS_Docker_Community_Edition_L1_Linux_Host_OS_v1.1.0.audit:55b64322410a460b9753fd1853b012bb.
1359. Manage sensitive data with Docker secrets, from https://docs.docker.com/engine/swarm/secrets/#:~:text=You%20can%20use%20secrets%20to,SSH%20keys.
1360. John Walsh (30 Nov 2020), Container Security, from https://developer.cyberark.com/blog/container-security-best-practices-for-secrets-management-in-containerized-environments/.
1361. Robert Kimani (09 Oct 2023), Container Security and the Importance of Secure Runtimes, from https://thenewstack.io/container-security-and-the-importance-of-secure-runtimes/.
1362. Everything you need to know about Container Runtime Security, from https://snyk.io/learn/container-security/runtime-security/.
1363. Restrict container privileges, from https://docs.aws.amazon.com/whitepapers/latest/security-practices-multi-tenant-saas-applications-eks/restrict-container-privileges.html.
1364. John Jainschigg (06 Feb 2023), How to Simplify Kubernetes Updates and Reduce Risk, from https://thenewstack.io/how-to-simplify-kubernetes-updates-and-reduce-risk/.

Module 12 Enterprise Cloud Network Security

1365. Microsoft Azure (October 18, 2019) Azure infrastructure security, from https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

1366. Teju Shymansundar (June 21, 2018) What is ADFS?, from https://www.okta.com/blog/2018/06/what-is-adfs/

1367. Microsoft (December 5, 2018) What is password hash synchronization with Azure AD?, from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs

1368. Microsoft Azure (October 28, 2019) Azure Identity Management and access control security best practices, from https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices

1369. Adam (January 13, 2017) How to sync on-premises Active Directory to Azure Active Directory with Azure AD Connect?, from https://www.codetwo.com/admins-blog/how-to-sync-on-premises-active-directory-to-azure-active-directory-with-azure-ad-connect/#targetText=To%20open%20Synchronization%20Service%20Manager,can%20monitor%20the%20synchronization%20progress.

1370. How to Deploy Active Directory Federation Services (ADFS) on Windows Server 2019, from https://www.systemsitpro.com/2019/03/Deploy-ADFS-2019.html

1371. Microsoft (April 16, 2019) Azure Active Directory Seamless Single Sign-On: Quick start, from https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

1372. Mike O. Villegas (January 26, 2016) How to limit privileged accounts and boost security, from https://searchsecurity.techtarget.com/tip/How-to-limit-privileged-accounts-and-boost-security

1373. Microsoft (February 7, 2020) Assign Azure AD roles in Privileged Identity Management, from https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=previous

1374. Microsoft Azure (December 7, 2017) Azure Security Documentation, http://cloudarchitects.pl/wp-content/uploads/2018/02/Azure-Security.pdf

1375. Microsoft Azure (May 26, 2017) Configuring TLS for an application in Azure, from https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-configure-ssl-certificate-portal

1376. Yousef Khalidi (2017) Azure Network Security, from https://azure.microsoft.com/nl-nl/blog/azure-network-security/

1377. Microsoft (March 15, 2016) Manage endpoint access control lists using PowerShell in the classic deployment model, from https://docs.microsoft.com/en-us/previous-versions/azure/virtual-network/virtual-networks-acl-powershell

1378. Microsoft Azure (March 9, 2020) Quickstart: Direct web traffic with Azure Application Gateway - Azure portal, from https://docs.microsoft.com/en-us/azure/application-gateway/quick-create-portal

1379. Microsoft Azure (March 11, 2019) Tutorial: Load balance internet traffic to VMs using the Azure portal, from https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal

1380. Microsoft Azure (February 21, 2020) Tutorial: Deploy and configure Azure Firewall using the Azure portal, from https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

1381. Microsoft Azure (March 9, 2020) Azure data security and encryption best practices, from https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

1382. Microsoft Azure (March 26, 2019) Microsoft Antimalware for Azure Cloud Services and Virtual Machines, from https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware

1383. Tutorialspoint Microsoft Azure - Monitoring Virtual Machines, from https://www.tutorialspoint.com/microsoft_azure/microsoft_azure_monitoring_virtual_machines.htm

1384. Microsoft Azure, Network Watcher, from https://azure.microsoft.com/en-in/services/network-watcher/

1385. Microsoft Azure (April 24, 2018) What is Azure Network Watcher? from https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

1386. Arunvignesh Venkatesh (August 31, 2017) Cloud Computing Security: Provider & Consumer Responsibilities, from https://www.mindtree.com/blog/cloud-computing-security-provider-consumer-responsibilities

1387. Google Cloud, Cloud IAM, from https://cloud.google.com/iam/docs/overview

1388. Inflobox, Creating GCP Service Account, from https://docs.infoblox.com/display/vniosgcp/Creating+GCP+Service+Account

1389. Google Cloud, Restricting Service Account Usage, from https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts

1390. Google Cloud, Management Tools, from https://cloud.google.com/logging/docs/access-control

1391. Google Cloud, Cloud Key Management Service, from https://cloud.google.com/kms

1392. Google Cloud, Google Security Model, from https://cloud.google.com/security/overview

1393. Google Cloud, Cloud Audit Logs, from https://cloud.google.com/logging/docs/audit

1394. Google Cloud, Monitoring audit logging information, from https://cloud.google.com/monitoring/audit-logging

1395. Google Cloud, Cloud Logging, from https://cloud.google.com/logging

1396. Google Cloud, Compliance Resource Center, from https://cloud.google.com/security/compliance

1397. Google Cloud (January 2017) Google Infrastructure Security Design Overview, from https://cloud.google.com/security/infrastructure/design/

1398. Margaret Rouse, identity and access management (IAM), from https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system.

1399. James A. Martin, What is IAM? Identity and access management explained, from https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html.

1400. Margaret Rouse, encryption key management, from https://searchdatabackup.techtarget.com/definition/encryption-key-management.
1401. Stratoscale, Security in Cloud Networking: FW, ACLs and More, from https://www.stratoscale.com/blog/data-center/security-cloud-networking-fw-acls/.
1402. Natalie Boyd, Achieving Network Security in Cloud Computing, from https://www.sdxcentral.com/cloud/definitions/achieving-network-security-in-cloud-computing/.
1403. Top 6 Methods to Protect Your Cloud Data from Hackers, from https://www.idexcel.com/blog/top-6-methods-to-protect-your-cloud-data-from-hackers/.
1404. Naomi Assaraf, 5 Safety Concerns with Cloud Data Storage, Answered, from https://blog.cloudhq.net/5-safety-concerns-with-cloud-data-storage-answered/.
1405. 7 Effective Tips to Secure Your Data in the Cloud, from https://hackernoon.com/7-effective-tips-to-secure-your-data-in-the-cloud-820bfe438d2.
1406. Ed Moyle, 3 best practices for cloud security monitoring, from https://searchcloudsecurity.techtarget.com/tip/Cloud-security-monitoring-Challenges-and-guidance.
1407. 4 Best Practices for Today's Log Management, from https://www.cloudaccess.com/cloud-based-log-management/.
1408. MIKE MASON, Key Considerations for Compliance in the Cloud, from https://www.corporatecomplianceinsights.com/key-considerations-compliance-cloud/.
1409. Natalie Boyd, Cloud Computing Security Architecture for IaaS, SaaS, and PaaS, from https://www.sdxcentral.com/cloud/defi.nitions/cloud-computing-security-architecture/.
1410. Best practices for enterprise organizations, from https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations.
1411. John Martinez, 8 Google Cloud Security Best Practices, from https://blog.palo, altonetworks.com/2019/04/8-google-cloud-security-best-practices/.
1412. STUART SCOTT, AWS Shared Responsibility Model: Cloud Security, from https://cloudacademy.com/blog/aws-shared-responsibility-model-security/.
1413. Shared Responsibility Model, from https://aws.amazon.com/compliance/shared-responsibility-model/.
1414. AWS Shared Security Model, from https://www.barracuda.com/glossary/aws-shared-security-model.
1415. Kai Zhao, New in IAM: Quickly Identify When an Access Key Was Last Used, from https://aws.amazon.com/blogs/security/new-in-iam-quickly-identify-when-an-access-key-was-last-used/.
1416. Getting Credential Reports for Your AWS Account, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_getting-report.html#getting-credential-reports-console.,
1417. Rob Moncur, New Information in the AWS IAM Console Helps You Follow IAM Best Practices, from https://aws.amazon.com/blogs/security/newly-updated-features-in-the-aws-iam-console-help-you-adhere-to-iam-best-practices/.
1418. Managing Access Keys for IAM Users, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html.
1419. IAM Best Practices, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html.
1420. Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-ec2.html.
1421. Lock Away Your AWS Account Root User Access Keys, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials.
1422. Enabling MFA Devices, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable.html.
1423. Zaher Dannawi, How to Enable MFA Protection on Your AWS API Calls, from https://aws.amazon.com/blogs/security/how-to-enable-mfa-protection-on-your-aws-api-calls/.
1424. Lock Away Your AWS Account Root User Access Keys, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials.
1425. STUART SCOTT, AWS Security: Identity and Access Management (IAM), from https://cloudacademy.com/blog/aws-security-identity-and-access-management-iam/.
1426. Setting an Account Password Policy for IAM Users, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html.
1427. Lock Away Your AWS Account Root User Access Keys, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials.
1428. Action Summary (List of Resources), from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_understand-action-summary.html.
1429. Service Summary (List of Actions), from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_understand-service-summary.html.
1430. Policy Summary (List of Services), from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_understand-policy-summary.html.
1431. Lock Away Your AWS Account Root User Access Keys, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials.
1432. AWS Managed Policies, from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies.
1433. Brad Lyman, An Easier Way to Manage Your Policies, from https://aws.amazon.com/blogs/security/an-easier-way-to-manage-your-policies/.

1434. Create Individual IAM Users, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users.
1435. AWS Managed Policies, from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_managed-vs-inline.html#aws-managed-policies.
1436. Creating Your First IAM Admin User and Group, from https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html.
1437. BethChimeAWS, Amazon Chime actions for IAM policies, from https://answers.chime.aws/articles/317/amazon-chime-actions-for-iam-policies.html.
1438. Adding and Removing Users in an IAM Group, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_groups_manage_add-remove-users.html.
1439. Create Individual IAM Users, from https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#create-iam-users.
1440. Rob Moncur, Now Create and Manage Users More Easily with the AWS IAM Console, from https://aws.amazon.com/blogs/security/now-create-and-manage-users-more-easily-with-the-aws-iam-console/.
1441. Enabling MFA Devices, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable.html.
1442. Changing the AWS Account Root User Password, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_change-root.html.
1443. Jeff Barr, IAM: AWS Identity and Access Management – from Now Generally Available, https://aws.amazon.com/blogs/aws/iam-identity-access-management/.
1444. Overview of Access Management: Permissions and Policies, from https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_access-management.html.
1445. AWS IAM features, from https://aws.amazon.com/iam/features/.
1446. AWS IAM, from https://www.simplilearn.com/aws-iam-tutorial-article.
1447. The AWS Account Root User, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html.
1448. Roles Terms and Concepts, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_terms-and-concepts.html.
1449. Creating a Role to Delegate Permissions to an IAM User, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user.html.
1450. Abhishek Pandey, Introducing an Easier Way to Delegate Permissions to AWS Services: Service-Linked Roles, from https://aws.amazon.com/blogs/security/introducing-an-easier-way-to-delegate-permissions-to-aws-services-service-linked-roles/.
1451. Using Temporary Credentials With AWS Resources, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html.
1452. Creating an IAM User in Your AWS Account, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html.
1453. Finding Unused Credentials, from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_finding-unused.html.
1454. Managing Access Keys (Console), from https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_CreateAccessKey.
1455. NITHEESH POOJARY, AWS IAM: How to Master Amazon Authentication in 5 Steps, from https://cloudacademy.com/blog/aws-iam-security/.
1456. Configuring and Using Access Logs, from https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html.
1457. Choosing an Amazon S3 Bucket for Your Access Logs, from https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html#access-logs-choosing-s3-bucket.
1458. What Is AWS CloudTrail?, from https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html.
1459. AWS CloudTrail features, from https://aws.amazon.com/cloudtrail/features/.
1460. AWS Config features, from https://aws.amazon.com/config/features/.
1461. Amazon S3 Features, from https://aws.amazon.com/s3/features/?nc=sn&loc=2.
1462. How do you protect your data at rest?, from https://wa.aws.amazon.com/wat.question.SEC_9.en.html.
1463. Ken Beer, Ryan Holland, Encrypting Data at Rest, from https://d1.awsstatic.com/whitepapers/AWS_Securing_Data_at_Rest_with_Encryption.pdf.
1464. AWS Security Best Practices, from https://d0.awsstatic.com/whitepapers/aws-security-best-practices.pdf.
1465. How do you classify your data?, from https://wa.aws.amazon.com/wat.question.SEC_8.en.html.
1466. Amazon Macie, from https://aws.amazon.com/macie/?ref=wellarchitected.
1467. Amazon S3-Managed Encryption Keys (SSE-S3), from https://docs.aws.amazon.com.
1468. AWS KMS-Managed keys (SSE-KMS), from https://docs.aws.amazon.com.
1469. Customer-provided keys (SSE-C), from https://docs.aws.amazon.com.
1470. Bouncy Castle, from http://www.bouncycastle.org/.
1471. OpenSSL, from https://www.openssl.org/.
1472. Ken Beer and Ryan Holland, Securing Data at Rest with Encryption, from https://d0.awsstatic.com/whitepapers/aws-securing-data-at-rest-with-encryption.pdf.
1473. What Is AWS Certificate Manager?, from https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html.
1474. Services Integrated with AWS Certificate Manager, from https://docs.aws.amazon.com/acm/latest/userguide/acm-services.html.

1475. Stephen Schmidt, Introducing s2n, a New Open Source TLS Implementation, from https://aws.amazon.com/blogs/security/introducing-s2n-a-new-open-source-tls-implementation/.
1476. Lee Atkinson, How to Help Achieve Mobile App Transport Security (ATS) Compliance by Using Amazon CloudFront and AWS Certificate Manager, from https://aws.amazon.com/blogs/security/how-to-help-achieve-mobile-app-transport-security-compliance-by-using-amazon-cloudfront-and-aws-certificate-manager/.
1477. Jeff Barr, New – AWS Certificate Manager – Deploy SSL/TLS-Based Apps on AWS, from https://aws.amazon.com/blogs/aws/new-aws-certificate-manager-deploy-ssltls-based-apps-on-aws/.
1478. Amazon Virtual Private Cloud, from https://aws.amazon.com/vpc/.
1479. AWS Security Best Practices, from https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf.
1480. Working with Security Groups, from https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#WorkingWithSecurityGroups.
1481. Jeff Barr, New – Descriptions for Security Group Rules, from https://aws.amazon.com/blogs/aws/new-descriptions-for-security-group-rules/.
1482. STUART SCOTT, AWS Security Groups: Instance Level Security, from https://cloudacademy.com/blog/aws-security-groups-instance-level-security/.
1483. Working with Network ACLs, from https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#nacl-tasks.
1484. AWS Direct Connect, from https://aws.amazon.co.m/directconnect/.
1485. AWS Direct Connect, from https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf.
1486. Amazon Web Services - Direct Connect, from https://www.tutorialspoint.com/amazon_web_services/amazon_web_services_direct_connect.htm.
1487. DMZ (computing), from https://en.wikipedia.org/wiki/DMZ_(computing).
1488. AWS VPC Subnets – in Layperson's Terms, from https://www.infoq.com/articles/aws-vpc-explained/.
1489. AWS Firewalls, from https://www.barracuda.com/glossary/aws-firewall.
1490. Route Tables, from https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html.
1491. Configuring DNS routing for a new domain, from https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-configuring-new-domain.html.
1492. Controlling VPC Egress Traffic, from https://aws.amazon.com/answers/networking/controlling-vpc-egress-traffic/.
1493. Jeff Barr , Amazon S3 Block Public Access – Another Layer of Protection for Your Accounts and Buckets, from https://aws.amazon.com/blogs/aws/amazon-s3-block-public-access-another-layer-of-protection-for-your-accounts-and-buckets/.
1494. AWS Security – Storage Services, from https://d1.awsstatic.com/whitepapers/Security/Security_Storage_Services_Whitepaper.pdf.
1495. Amazon S3 Features, from https://aws.amazon.com/s3/features/?nc=sn&loc=2.
1496. How Do I Add Metadata to an S3 Object?, from https://docs.aws.amazon.com/AmazonS3/latest/user-guide/add-object-metadata.html.
1497. AWS Tagging Strategies, from https://aws.amazon.com/answers/account-management/aws-tagging-strategies/.
1498. Alexander Watson, Classify sensitive data in your environment using Amazon Macie, from https://aws.amazon.com/blogs/security/classify-sensitive-data-in-your-environment-using-amazon-macie/.
1499. How AWS Config Works, from https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html.
1500. Track your resource configuration changes with AWS Config, from https://blog.cloudthat.com/track-your-resource-configuration-and-changes-with-aws-config/.
1501. AWS Well-Architected Framework, from https://d0.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf?ref=wellarchitected.
1502. Parveen, AWS, Google and Microsoft Azure Security Checklist, from https://www.xenonstack.com/blog/aws-google-azure-security/.

Module 13 Enterprise Wireless Network Security

1503. What is WiFi?, from http://www.scambusters.org/wifi.html.
1504. Paul Asadoorian (August 27th, 2009), A "Rogue" Access Point, https://www.tenable.com/blog/using-nessus-to-discover-rogue-access-points.
1505. White Paper Summary — Enterprise Approaches to Detecting Rogue Wireless LANs, from http://www.airdefense.net/eNewsletters/rogue_feature.shtm.
1506. SNMP Detection Utility, from http://www.mcafee.com/in/downloads/free-tools/snscan.aspx.
1507. Wireless network, from https://en.wikipedia.org/wiki/Wireless_network#Difficulties.
1508. Types of Wireless Networks, from http://computernetworkingnotes.com/wireless-networking-on-cisco-router/types-of-wireless-networks.html.
1509. Wireless Network, from https://www.techopedia.com/definition/26186/wireless-network.
1510. Wireless technology, from https://www.nibusinessinfo.co.uk/content/pros-and-cons-wireless-networking.
1511. Vangie Beal, Bluetooth, from http://www.webopedia.com/TERM/B/bluetooth.html.
1512. IEEE 802.11i-2004, from https://en.wikipedia.org/wiki/IEEE_802.11i-2004.
1513. 802.11i, from http://searchmobilecomputing.techtarget.com/definition/80211i.
1514. Computer Networks – options, from http://www.rdcs.com/network-options.htm.
1515. Alex Lane, 8TH FEB 2012, How to extend your home network, from https://recombu.com/digital/article/how-to-extend-your-home-network_M10028.html.

1516. Sharon Cobb, Wireless Transmission, from http://slideplayer.com/slide/6088293/.
1517. Creating one WiFi network with multiple access points, from https://www.savjee.be/2012/10/creating-one-WiFi-network-with-multiple-access-points/.
1518. How to setup multiple access points, from http://www.tomshardware.com/forum/27151-43-setup-multiple-access-points.
1519. Network Use Guide, from https://www.waseda.jp/navi/e/network/wireless.html.
1520. Bradley Mitchell, Finding and Using Wi-Fi Hot Spots, from http://compnetworking.about.com/od/wirelesshotspots/a/wifihotspots.htm.
1521. Mobile broadband modem, from https://en.wikipedia.org/wiki/Mobile_broadband_modem#3G.
1522. Hotspot (Wi-Fi)https://en.wikipedia.org/wiki/Hotspot_(Wi-Fi).
1523. access point, from http://searchmobilecomputing.techtarget.com/definition/access-point.
1524. Wireless access point, from https://en.wikipedia.org/wiki/Wireless_access_point.
1525. Dec 5, 2002, Wireless Networking NTK - Product Types, from http://www.tomsguide.com/us/wireless-networking-ntk,review-101-2.html.
1526. IEEE 802.11i-2004, from https://en.wikipedia.org/wiki/IEEE_802.11i-2004.
1527. Simplifying WPA2-Enterprise and 802.1X, from https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/.
1528. 02/25/201, What is WEP wireless encryption?, from http://kb.netgear.com/app/answers/detail/a_id/1141/~/what-is-wep-wireless-encryption%3F.
1529. Wired Equivalent Privacy, from https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.
1530. Wired Equivalent Privacy (WEP), from http://searchsecurity.techtarget.com/definition/Wired-Equivalent-Privacy.
1531. Wi-Fi Security, http://etutorials.org/Microsoft+Products/windows+xp+unwired/ Chapter+4.+Communicating+Securely/4.5+Wi-Fi+Security/.
1532. How does WEP wireless security work?, from http://security.stackexchange.com/questions/17434/how-does-wep-wireless-security-work.
1533. David B. Jacobs, Wireless security -- How WEP encryption works, from http://searchnetworking.techtarget.com/tip/Wireless-security-How-WEP-encryption-works.
1534. Overview of the Wi-Fi Protected Access (WPA) security update in Windows XP, from https://support.microsoft.com/en-us/kb/815485.
1535. Wi-Fi Protected Access, from Wi-Fi Protected Access, from https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.
1536. Wi-Fi Protected Access (WPA), http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access.
1537. May/Aug. 2008, Basic security measures for IEEE 802.11 wireless networks, from http://www.scielo.org.co/scielo.php?pid=S0120-56092008000200012&script=sci_arttext.
1538. Real-time Traffic over WLAN Security, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/RToWLAN/CCVP_BK_R7805F20_00_rtowlan-srnd/CCVP_BK_R7805F20_00_rtowlan-srnd_chapter_0100.html.
1539. Xiuzhen Cheng, Wireless and Mobile Security – Key Hierarchies for WPA and RSN, from http://slideplayer.com/slide/9095623/.
1540. 802.1X Port-Based Authentication HOWTO, from http://www.tldp.org/HOWTO/8021X-HOWTO/intro.html.
1541. The differences between WPA-Personal and WPA-Enterprise, from http://www.tp-link.com/en/FAQ-500.html.
1542. Bradley Mitchell (March 31, 2016), What is WPA2?, from http://compnetworking.about.com/od/wirelesssecurity/f/what-is-wpa2.htm.
1543. Cisco Unified Wireless Network Architecture—Base Security Features, from http://www.cisco.com/ c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch4_Secu.html#wp1019004.
1544. HOST-TO-NETWORK LAYER PROTOCOLS , from http://www.fidis.net/resources/fidis-deliverables/hightechid/int-d37003/doc/12/.
1545. Authentication Types for Wireless Devices, from http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html.
1546. Authentication Types for Wireless Devices, from ftp://ftp.scv.si/vss/uros_sonjak/Cisco/WLAN/SecurityAuthenticationTypes.pdf.
1547. Jim Burns (Apr 3, 2003), How 802.1x authentication works, from http://www.computerworld.com/article/2581074/ mobile-wireless/how-802-1x-authentication-works.html.
1548. Andrew Z. Tabona (4 Aug. 2005), An Overview of Wireless Network Security, from http://www.windowsnetworking.com/ articles-tutorials/wireless-networking/Overview-Wireless-Network-Security.html.
1549. How to Use Wireshark to Capture, Filter and Inspect Packets, from http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/.
1550. Mallikarjun Hangargi, Business Need for Security Denail of ervice Attacks in Wireless Networks, from https://dl.packetstormsecurity.net/papers/wireless/DoS_attacks_in_wireless_networks.pdf.
1551. WiFi Security – Do's and Don'ts, from http://www.techspeak.ca/wifi-security-dos-and-donts/.
1552. Tips For Securing Your Wireless Connection, from https://www.sophos.com/en-us/security-news-trends/best-practices/wi-fi.aspx.
1553. http://www.networkworld.com/article/2182865/wireless/wi-fi-security-do-s-and-don-ts.html.
1554. Eric Geier Nov 7, 2011,Wi-Fi security do's and don'ts 11 tips for protecting your wireless networks, from http://www.techspeak.ca/wifi-security-dos-and-donts/.
1555. Pablo Estrada June 30, 2011, 10 BEST PRACTICES FOR DESIGNING YOUR EVENT WI-FI DEPLOYMENT, from https://meraki.cisco.com/blog/2011/06/10-best-practices-for-designing-your-event-wi-fi-deployment/.
1556. Wireless Network Vulnerability Assessment, from https://www.secnap.com/products-services/security-services/internal-vulnerability-assessment/.
1557. ZENworks Endpoint Security Management, from https://www.novell.com/products/zenworks/endpointsecuritymanagement/features/personal-firewall.html.

1558. Wireless Access Point Protection, from https://www.securitymetrics.com/blog/wireless-access-point-protection-finding-rogue-wi-fi-networks.

1559. 09 Dec 2011, WIDS WIPS 101: Wireless Intrusion Detection And Prevention Systems Wireless IDS IPS, from https://www.thesecurityblogger.com/wids-wips-101-wireless-intrusion-detection-and-prevention-systems-wireless-ids-ips/#:~:text=WIDS%20are%20wireless%20access%20points,rather%20than%20automatically%20killing%20them.

1560. Brad Hale (2012), Monitoring Rogue Access points, from https://thwack.solarwinds.com/resources/b/geek-speak/posts/monitoring-rogue-access-points-in-your-wlan#:~:text=SolarWinds%20Network%20Performance%20Monitor%20(NPM,scanning%20wireless%20controllers%20and%20devices.

1561. Mayank Dham (31 Jul 2023), MAC Filtering, from https://www.prepbytes.com/blog/operating-system/mac-filtering/.

1562. Warchalking in Wireless Networks, from https://www.geeksforgeeks.org/warchalking-in-wireless-networks/.

1563. What is Warchalking, from https://www.techslang.com/definition/what-is-warchalking/.

1564. Warchalking in Wireless Networks, from https://www.javatpoint.com/warchalking-in-wireless-networks.

1565. Wi-Fi Easy Connect, from https://source.android.com/docs/core/connect/wifi-easy-connect.

1566. Wi-Fi Easy Connect, from https://docs.espressif.com/projects/esp-idf/en/latest/esp32s3/api-reference/network/esp_dpp.html#:~:text=Wi%2DFi%20Easy%20ConnectTM%2C%20also%20known%20as%20Device%20Provisioning,as%20scanning%20a%20QR%20Code.

Module 14 Network Traffic Monitoring and Analysis

1567. Rich Macfarlane, Packet Capture & Traffic Analysis with Wireshark from http://www.soc.napier.ac.uk/~cs342/ CSN11102/Lab5.pdf.

1568. CHRIS SANDERS, PRACTICAL PACKET ANALYSIS USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS, from http://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf.

1569. WIRESHARK DISPLAY FILTERS, from http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf.

1570. Bobby Rogers, TCP/IP Packet Analysis Course, from http://www.vtc.com/products/TCP-IP-Packet-Analysis-Tutorials.htm.

1571. Packet Sniffing, from http://lists.thedatalist.com/pages/Packet_Sniffing.htm.

1572. Ishan Bansal (January 16, 2011), 5 BEST FREE NETWORK PACKET SNIFFER, from http://www.ilovefreesoftware.com/16/featured/5-best-free-network-packet-sniffer.html.

1573. Detect/Analyze Scanning Traffic Using Wireshark, from http://www.koenig-solutions.com/documents/PenTestExtra-06-2013.pdf.

1574. Alisha Cecil, A Summary of Network Traffic Monitoring and Analysis Techniques, from http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf.

1575. Karen Kent Frederick (December 19, 2001), Network Intrusion Detection Signatures, from http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-part-one.

1576. Network Traffic Analysis, from https://www.techopedia.com/definition/29976/network-traffic-analysis.

1577. Intrusion Prevention Fundamentals: Signatures and Actions, from http://searchsecurity.techtarget.com/feature/Intrusion-Prevention-Fundamentals-Signatures-and-Actions.

1578. James Foster, IDS: Signature versus anomaly detection, from http://searchsecurity.techtarget.com/tip/IDS-Signature-versus-anomaly-detection.

1579. Sagar N. Shah, Ms. Purnima Singh (28-12-2012), Signature-Based Network Intrusion Detection System Using SNORT And WINPCAP, from http://www.ijert.org/view-pdf/1923/signature-based-network-intrusion-detection-system-using-snort-and-winpcap.

1580. Karen Kent Frederick (February 19, 2002), Network Intrusion Detection Signatures, from http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-part-three.

1581. Catherine Paquet (Jun 8, 2009), Network Security Using Cisco IOS IPS, from http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=5.

1582. Gerhard Munz, Nico Weber, Georg Carle, Signature Detection in Sampled Packets from http://www.net.in.tum.de/fileadmin/TUM/members/ muenz/documents/muenz07signature.pdf.

1583. Packet Capture, from https://www.techopedia.com/definition/25333/packet-capture.

1584. Otusile Oluwabukola, Awodele Oludele, A.C Ogbonna, Ajeagbu Chigozirim, and Anyeahie Amarachi, A Packet Sniffer (PSniffer) Application for Network Security in Java, from http://iisit.org/Vol10/IISITv10p389-400Oluwabukola0037.pdf.

1585. Aniket Amdekar (09 feb 2011), Capturing network communication packets with Wireshark Utility, from http://www.symantec.com/connect/articles/capturing-network-communication-packets-wireshark-utility.

1586. Ulf Lamping, Richard Sharpe, Ed Warnicke, Wireshark User's Guide For Wireshark 2.1, from https://www.wireshark.org/download/docs/user-guide-us.pdf.

1587. Laura Chappell (May 13, 2008), How to - Wireshark Training: More Statistics, from https://www.youtube.com/watch?v=hrExIIJYJho.

1588. Gerald Combs and Laura Chappell , Introduction to Wireshark 2.0 w/, from https://www.youtube.com/watch?v=rLfYuO6pdVA.

1589. Filtering while capturing, from https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html.

1590. 3 August 2015, PCAP-FILTER, from http://www.tcpdump.org/manpages/pcap-filter.7.html.

1591. Filtering packets while viewing, from https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html.

1592. Michael Brandenburg, How to set a network performance baseline for network monitoring, from http://searchnetworking.techtarget.com/How-to-set-a-network-performance-baseline-for-network-monitoring .

1593. Analysis of Network Packets, from http://www.iitg.ernet.in/cse/ISEA/isea_PPT/ISEA_02_09/Analysis%20of%20Network%20Packets.pdf.
1594. October 29, 2010, Developing a Network Performance Baseline, from http://www.atlantixglobal.com/network-performance-baseline/?pg=6.
1595. Karen Kent Frederick (03 Nov 2010), Abnormal IP Packets, from http://www.symantec.com/connect/articles/abnormal-ip-packets.
1596. TCP Message (Segment) Format, from http://www.tcpipguide.com/free/t_TCPMessageSegmentFormat-3.htm.
1597. SYN and FIN Bit Set at the Same Time, from http://kb.juniper.net/InfoCenter/index?page=content&id=KB5801&actp=search.
1598. Internet Control Message Protocol (ICMP), from http://www.erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/icmp.html .
1599. ICMP Common Message Format and Data Encapsulation, from http://www.tcpipguide.com/free/t_ICMPCommonMessageFormatandDataEncapsulation.htm.
1600. Active FTP vs. Passive FTP, a Definitive Explanation, from http://slacksite.com/other/ftp.html .
1601. What is File Transfer Protocol (FTP)?, from http://whatismyipaddress.com/ftp.
1602. Computer network and security threat, from http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/reconnaissance-attacks.html.
1603. Margaret Rouse (April 2012), active reconnaissance, from http://whatis.techtarget.com/definition/active-reconnaissance.
1604. Margaret Rouse (April 2012), passive reconnaissance, from http://whatis.techtarget.com/definition/passive-reconnaissance.
1605. Unauthorized access Attack, from http://itsecurity.telelink.com/unauthorized-access-attack/.
1606. Margaret Rouse (July 2006), Cleartext, from http://whatis.techtarget.com/definition/cleartext.
1607. Establishing an FTP Connection from the Command Prompt, from http://kb.globalscape.com/ KnowledgebaseArticle10224.aspx.
1608. How to Use Wireshark to Capture, Filter and Inspect Packets, from http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/.
1609. June 19, 2014, What You Must Know About OS Fingerprinting, from http://resources.infosecinstitute.com/must-know-os-fingerprinting/.
1610. What is Ping Sweep, from https://www.hackingloops.com/what-is-ping-sweep.html.
1611. Address Resolution Protocol (ARP), from http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP.
1612. Anim Saxena (03/10/2014), Advanced Attacks using TCP/IP for Scanning, from https://supportforums.cisco.com/ blog/153536.
1613. Port Scanning Techniques, from https://nmap.org/book/man-port-scanning-techniques.html.
1614. December 07, 2015 , TCP Xmas Scan, from https://capec.mitre.org/data/definitions/303.html.
1615. Detect password cracking attempts, from https://www.safaribooksonline.com/library/view/wireshark-network-security/9781784393335/ch03s04.html.
1616. Password Cracking, from https://www.techopedia.com/definition/4044/password-cracking.
1617. dictionary attack, from http://www.webopedia.com/TERM/D/dictionary_attack.html.
1618. What is a POP3?, from http://whatismyipaddress.com/pop3.
1619. File Transfer Protocol (FTP), from http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol.
1620. Sniffing, from http://swissen.in/sniffing.php.
1621. What is MAC flooding attack and How to prevent MAC flooding attack, from http://www.omnisecu.com/ccna-security/what-is-mac-flooding-attack-how-to-prevent-mac-flooding-attack.php.
1622. Address Resolution Protocol Poisoning (ARP Poisoning), from https://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp-poisoning.
1623. [Wireshark-users] Duplicate IPs, from https://www.wireshark.org/lists/wireshark-users/201006/msg00234.html.
1624. Trivial File Transfer Protocol, from https://wiki.wireshark.org/TFTP.md.
1625. Howard Poston (11 Feb 2020), Network traffic analysis for IR: TFTP with Wireshark, from https://resources.infosecinstitute.com/topic/network-traffic-analysis-for-ir-tftp-with-wireshark/.
1626. SNMP, from https://wiki.wireshark.org/SampleCaptures#snmp.
1627. Encrypted UDP based FTP with multicast (UFTP), from https://wiki.wireshark.org/Protocols/uftp.md.
1628. Dynamic Host Configuration Protocol (DHCP), from https://wiki.wireshark.org/DHCP.
1629. 14 May 2021, VLAN hoping, from https://www.infosecmatter.com/detecting-network-attacks-with-wireshark/#vlan-hoping.
1630. VLAN Hopping, from https://networklessons.com/cisco/ccnp-switch/vlan-hopping.
1631. What is VLAN Hopping and How it is Performed, from https://zindagitech.com/what-is-vlan-hopping-and-how-it-is-performed/.
1632. Prabhat Kumar Tomar, What is a TLS/SSL Port, from https://www.encryptionconsulting.com/what-is-a-tls-ssl-port/.
1633. Prateek Gianchandani (25 Nov 2014), Android Application hacking with Insecure Bank Part 1, from https://resources.infosecinstitute.com/topic/decrypting-ssl-tls-traffic-with-wireshark/.
1634. Kerberos Traffic from Unusual Process, from https://www.elastic.co/guide/en/security/current/kerberos-traffic-from-unusual-process.html.
1635. Client deauthentication, from https://www.infosecmatter.com/detecting-network-attacks-with-wireshark/#client-deauthentication.
1636. Subham Datta (30 April 2023), Wireless Disassociation Attacks, from https://www.baeldung.com/cs/wireless-disassociation-attacks.
1637. MDK3, from https://en.kali.tools/?p=34.
1638. Wireshark/HTTPS, from https://en.wikiversity.org/wiki/Wireshark/HTTPS.

1639. Margaret Rouse (18 Jan 2017), Network Behavior Anomaly Detection, from https://www.techopedia.com/definition/16119/network-behavior-anomaly-detection-nbad#site-header.
1640. Hossein Ashtari (28 Feb 2022), What Is Network Behavior Anomaly Detection, from https://www.spiceworks.com/tech/networking/articles/network-behavior-anomaly-detection/.
1641. Tarem Ahmed, Machine Learning Approaches to Network Anomaly Detection, from https://www.usenix.org/legacy/event/sysml07/tech/full_papers/ahmed/ahmed_html/sysml07CR_07.html.
1642. Network Anomaly Detection and Network Behavior Analysis, from https://www.flowmon.com/en/solutions/security-operations/network-behavior-analysis-anomaly-detection.
1643. Ying Zhao (23 Jun 2019), Network Anomaly Detection by Using a Time-Decay Closed Frequent Pattern, from https://www.mdpi.com/2078-2489/10/8/262.
1644. Anomaly Detection, from https://avinetworks.com/glossary/anomaly-detection/.
1645. Data processing, from https://www.britannica.com/technology/data-processing.
1646. Frequent Pattern Mining in Data Mining, from https://www.geeksforgeeks.org/frequent-pattern-mining-in-data-mining/.
1647. Security for your business is 100% our business, from https://www.cisco.com/site/us/en/products/security/security-analytics/secure-network-analytics/index.html.
1648. Cisco Secure Network Analytics (Stealthwatch), from https://www.cisco.com/c/en_hk/products/security/stealthwatch/index.html.
1649. 10 Dec 2020, Cisco Security Analytics White Paper, from https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/white-paper-c11-740605.html.
1650. Margaret Rouse (18 Jan 2017), Network Behavior Anomaly Detection, from https://www.techopedia.com/definition/16119/network-behavior-anomaly-detection-nbad#site-header.
1651. Daniel Hein, Network Behavior Analysis and Anomaly Detection, from https://solutionsreview.com/network-monitoring/network-behavior-analysis-and-anomaly-detection-the-basics/.
1652. Hossein Ashtari (28 Feb 2022), What Is Network Behavior Anomaly Detection, from https://www.spiceworks.com/tech/networking/articles/network-behavior-anomaly-detection/.
1653. Network Behavior Analytics, from https://docs.aviatrix.com/copilot/latest/network-security/network-anomalies.html.
1654. 8 Dec 2023, What's New in CoPilot, from https://docs.aviatrix.com/copilot/latest/aviatrix-overview/what-is-new.html.
1655. Security for your business is 100% our business, from https://www.cisco.com/site/us/en/products/security/security-analytics/secure-network-analytics/index.html.
1656. Anomalous user behavior, from https://www.manageengine.com/log-management/ueba/help/dashboard/ueba-dashboard-view.html.
1657. Keep track of your network's health and performance, from https://www.zabbix.com/network_monitoring.
1658. Search and Visualize Your Security Data, from https://www.rapid7.com/products/insightidr/use-cases/.
1659. AlienVault OSSIM is trusted by security professionals across the globe, from https://cybersecurity.att.com/products/ossim.
1660. Network anomaly detection system, from https://www.flowmon.com/en/products/software-modules/anomaly-detection-system.
1661. Network Traffic Analysis (NTA), from https://gurucul.com/products/network-traffic-analysis.
1662. 06 Jan 2023, QRadar Network Insights overview, from https://www.ibm.com/docs/en/qsip/7.5?topic=insights-qradar-network-overview.
1663. Flow-based network traffic monitoring for in-depth traffic analysis, from https://www.manageengine.com/products/netflow/.
1664. What is User Behavior Analytics, from https://www.manageengine.com/products/active-directory-audit/learn/what-is-user-behavior-analytics.html.
1665. User behavior analytics (UBA), from https://www.techtarget.com/searchsecurity/definition/user-behavior-analytics-UBA.
1666. Michael Buckbee (25 Feb 2022), What is User Behavior Analytics, from https://www.varonis.com/blog/what-is-user-behavior-analytics.
1667. An Introductory Guide to User Behavior Analytics, from https://www.softactivity.com/user-behavior-analytics/.
1668. What is user behavior analytics (UBA), from https://www.elastic.co/what-is/user-behavior-analytics.
1669. Ben Aston (24 Nov 2023), 17 Best User Behavior Analytics Tools in 2023, from https://theproductmanager.com/tools/best-user-behavior-analytics-tools/.
1670. Make your product metrics, sales, and customer success better, from https://creabl.com/.
1671. User Experience Eats Strategy for Breakfast, from https://www.userlytics.com/?r=prd-ubat.
1672. Deliver wow-worthy digital experiences, from https://www.pendo.io/?r=prd-ubat.
1673. Real User Monitoring, from https://www.datadoghq.com/product/real-user-monitoring/?r=prd-ubat.
1674. UEBA Definition, from https://www.fortinet.com/resources/cyberglossary/what-is-ueba.
1675. What is UEBA (user and entity behavior analytics), from https://www.ibm.com/topics/ueba.
1676. Chris Brook (31 May 2020), What is User and Entity Behavior Analytics, from https://www.digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more.
1677. 15 Sep 2020, What is User and Entity Behavior Analytics, from https://www.logpoint.com/en/blog/ueba-user-and-entity-behavior-analytics/.
1678. 06 Sep 2023, UBA vs UEBA - Decoding the Differences, from https://www.logsign.com/blog/ueba-vs-uba-decoding-the-differences/.
1679. USER ENTITY AND BEHAVIOR ANALYTICS, from https://www.dnif.it/en/ueba-user-entity-and-behavior-analytics.
1680. User and Entity Behavior Analytics, from https://www.securonix.com/products/ueba/.
1681. Get instant visibility into employee productivity and engagement, from https://www.activtrak.com.

1682. IBM Security QRadar SIEM, from https://www.ibm.com/in-en/products/qradar-siem.

1683. The world's leading AI-native platform for endpoint security, from https://www.crowdstrike.com/products/endpoint-security/.

Module 15 Network Logs Monitoring and Analysis

1684. Information Security Incident Management Policy, last modified: November 2017, https://www.hw.ac.uk/documents/information-security-incident-management.pdf.

1685. Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone, Computer Security Incident Handling Guide, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

1686. Christine Darville, Miguel De Bruycker, Cyber Security Incident Management Guide, https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf.

1687. Information Security Incident Reporting, last modified: June 29, 2016, https://spg.umich.edu/policy/601.25.

1688. The Definition of a Cyber Security incident, http://eweb.cabq.gov/CyberSecurity/Additional%20Security%20Documents/Reporting%20a%20Cyber%20Security%20incident.pdf.

1689. Margaret Rouse, Security Event, last modified: November 2016, https://whatis.techtarget.com/definition/security-event-security-incident.

1690. David Nathans, Designing and Building a Security Operations Center, last modified: 2015, http://index-of.es/Varios/David%20Nathans-Designing%20and%20Building%20Security%20Operations%20Center-Syngress%20(2014).pdf.

1691. Karen Kent, Murugiah Souppaya, Guide to Computer Security Log Management, last modified: September 2006, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf.

1692. Wang Wei, Importance of Logs and Log Management for IT Security, last modified: October 02, 2013, https://thehackernews.com/2013/10/importance-of-logs-and-log-management.html.

1693. OWASP Logging Project – Roadmap, https://www.owasp.org/images/archive/e/e0/20090807131642%21OWASP_Logging_Guide.pdf.

1694. Tom Goldsmith, Centre for the Protection of National Infrastructure Effective Log Management, last modified: April 02, 2014, https://www.ncsc.gov.uk/content/files/protected_files/document_files/2014-04-02-Effective%20Log%20Management.pdf.

1695. Gary Glover, The Importance of Log Management, last modified: October 03, 2018, https://www.securitymetrics.com/blog/importance-log-management.

1696. Log review and management, last modified: May 27, 2009, https://www.owasp.org/index.php/Log_review_and_management.

1697. Jason Creasey, Ian Glover, Cyber Security Monitoring and Logging Guide, last modified: 2015, https://www.crest-approved.org/wp-content/uploads/2015/05/Cyber-Security-Monitoring-Guide.pdf.

1698. Vikesh Tiwari, Part 1: Building a Centralized Logging Application, last modified: January 21, 2018, https://hackernoon.com/part-1-building-a-centralized-logging-application-5a537033da0a.

1699. Eventlog Key, last modified: May 31, 2018, https://docs.microsoft.com/en-us/windows/desktop/eventlog/eventlog-key.

1700. Toni Boger, Alexander Gillis, Windows event log, last modified: May 2018, https://searchwindowsserver.techtarget.com/definition/Windows-event-log.

1701. Shourjo Chakraborty, Introduction to Event Log Analysis Part 1 - Windows Forensics Manual 2018, last modified: 2018, https://lucideustech.blogspot.com/2018/09/introduction-to-event-log-analysis-part.html.

1702. Monitoring Windows Event Logs, https://download.manageengine.com/network-monitoring/monitoring-windows-eventlogs.pdf.

1703. Event Log File Format, last modified: March 31, 2018, https://docs.microsoft.com/en-us/windows/desktop/eventlog/event-log-file-format.

1704. Event Viewer, last modified: September 28, 2018, https://en.wikipedia.org/wiki/Event_Viewer.

1705. Chris Hoffman, What Is the Windows Event Viewer, and How Can I Use It, last modified: November 12, 2018, https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/.

1706. Windows Event Viewer, last modified: April 11, 2017, https://www.computerhope.com/jargon/e/evenview.htm.

1707. Shawn, How to Open and Use Event Viewer in Windows 7, last modified: April 23, 2012, https://www.sevenforums.com/tutorials/226084-event-viewer-open-use-windows-7-a.html.

1708. Event Types, last modified: May 31, 2018, https://docs.microsoft.com/en-us/windows/desktop/eventlog/event-types.

1709. Monitoring Windows Event Logs - A Tutorial, https://www.manageengine.com/network-monitoring/Eventlog_Tutorial_Part_I.html#need_for_monitoring.

1710. Windows Event Log Monitoring and Management with Nagios, https://www.nagios.com/solutions/windows-event-log-monitoring/.

1711. How to Diagnose System Problems with Event Viewer in Microsoft Windows 2000, last modified: July 13, 2010, https://support.microsoft.com/en-us/help/302542/how-to-diagnose-system-problems-with-event-viewer-in-microsoft-windows.

1712. Orin Thomas, How to Efficiently Search and Manage Event Log Data, last modified: January 04, 2010, https://www.itprotoday.com/devops-and-software-development/how-efficiently-search-and-manage-event-log-data.

1713. Greg Shultz, How to use custom views in Windows 10's Event Viewer, last modified: May 19, 2016, https://www.techrepublic.com/article/how-to-use-custom-views-in-windows-10s-event-viewer/.

1714. Lack Wallen, Viewing Linux Logs from the Command Line, last modified: July 18, 2018, https://www.linux.com/learn/sysadmin/viewing-linux-logs-command-line.

1715. Angela Stringfellow, What Are Linux Logs? How to View Them, Most Important Directories, and More, last modified: June 26, 2017, https://dzone.com/articles/what-are-linux-logs-how-to-view-them-most-importan.

1716. Marcel, 12 Critical Linux Log Files You Must be Monitoring, last modified: April 19, 2018, https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring/.

1717. What are Linux Logs? How to View Them, Most Important Directories, and More, last modified: June 23, 2017, https://stackify.com/linux-logs/.
1718. Vivek Gite, Linux Log Files, last modified: December 2017, https://linuxsecurityblog.com/2017/12/01/linux-log-files-lsb/.
1719. Raj Chandel, Understanding Log Analysis of Web Server, last modified: August 31, 2017, https://www.hackingarticles.in/understanding-log-analysis-web-server/.
1720. Ramesh Natarajan, 20 Linux Log Files that are Located under /var/log Directory, last modified: August 01, 2001, https://www.thegeekstuff.com/2011/08/linux-var-log-files/.
1721. Unix/ Linux - System Logging, https://www.tutorialspoint.com/unix/pdf/unix-system-logging.pdf.
1722. Akshay Rajput, grep command in Unix/Linux, https://www.geeksforgeeks.org/grep-command-in-unixlinux/.
1723. Mandeep Singh, less command in Linux with Examples, https://www.geeksforgeeks.org/less-command-linux-examples/.
1724. Pranav, Cat command in Linux with examples, https://www.geeksforgeeks.org/cat-command-linux-examples/.
1725. Akash Gupta, Tail command in Linux with examples, https://www.geeksforgeeks.org/tail-command-linux-examples/.
1726. Chris Hoffman, How to View the System Log on a Mac, last modified: July 9, 2018, https://www.howtogeek.com/356942/how-to-view-the-system-log-on-a-mac/.
1727. Mark Hurlow, Ryan R. Kubasiak, Forensically Sound Examination of a Macintosh (Part 2), last modified: June 21, 2007, https://macforensicslab.com/2007/06/21/forensically-sound-examination-macintosh-part-2/.
1728. Manual of printer administration information for the Common UNIX Printing, https://opensource.apple.com/source/cups/cups-87/doc/sam.shtml#ErrorLog.
1729. Alexander Fox, How to Read macOS Crash Reports to Troubleshoot Your MacSystem, last modified: March 23, 2018, https://www.maketecheasier.com/read-macos-crash-reports-troubleshoot-mac/.
1730. "Go to Folder" is the Most Useful Mac OS X Keyboard Shortcut for Power Users, last modified: August 31, 2011, http://osxdaily.com/2011/08/31/go-to-folder-useful-mac-os-x-keyboard-shortcut/.
1731. Laura Taylor, Read your firewall logs, last modified: July 5, 2001, https://www.zdnet.com/article/read-your-firewall-logs-5000298230/.
1732. Marcus J. Ranum, System Logging and Log Analysis, last modified: May 28, 2004, http://ranum.com/security/computer_security/archives/logging-notes.pdf.
1733. Rahuyl Saigal, How to Track Firewall Activity with the Windows Firewall Log, last modified: July 11, 2017, https://www.howtogeek.com/220204/how-to-track-firewall-activity-with-the-windows-firewall-log/.
1734. Interpreting the Windows Firewall Log, last modified: October 08, 2009, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc758040(v%3dws.10).
1735. Who's There? Firewall Advisor User's Guide, http://opendoor.biz/whosthere/ug/WTAppendix.html.
1736. Supriyo Biswas, An In-Depth Guide to iptables, the Linux Firewall, last modified: June 18, 2017, https://www.booleanworld.com/depth-guide-iptables-linux-firewall/.
1737. Marin Todorov, 25 Useful IPtable Firewall Rules Every Linux Administrator Should Know, last modified: March 01, 2016, https://www.tecmint.com/linux-iptables-firewall-rules-examples-commands/.
1738. Prithviraj S, Iptables Tutorial – Securing Ubuntu VPS with Linux Firewall, last modified: February 04, 2019, https://www.hostinger.in/tutorials/iptables-tutorial#gref.
1739. Korbin Brown, The Beginner's Guide to iptables, the Linux Firewall, last modified: July 03, 2017, https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/.
1740. Rahul, How to Enable Logging in Iptables on Linux, last modified: January 12, 2015, https://tecadmin.net/enable-logging-in-iptables-on-linux/.
1741. Cisco ASA 5500-X Series Next-Generation Firewalls, https://www.cisco.com/c/en_in/products/security/asa-5500-series-next-generation-firewalls/index.html.
1742. ASA 8.2: Packet Flow through an ASA Firewall, last modified: May 18, 2015, https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113396-asa-packet-flow-00.html.
1743. Ashutosh Patel, Key Features of the Cisco ASA Firewall, http://netfixpro.com/key-features-of-the-cisco-asa-firewall/.
1744. Andrew Froehlich, Cisco ASA firewall: Network security product overview, last modified: November 2015, https://searchnetworking.techtarget.com/feature/Cisco-ASA-firewall-Network-security-product-overview.
1745. Alok, Cisco ASA Packet Processing Algorithm, last modified: June 13, 2014, https://learningnetwork.cisco.com/docs/DOC-24239.
1746. Cisco ASA: Logging, https://www.grandmetric.com/knowledge-base/design_and_configure/how-to-configure-logging-on-cisco-asa/.
1747. Logging options on the Cisco ASA, last modified: March 11, 2013, https://vegaskid.net/2013/03/logging-options-on-the-cisco-asa/.
1748. David Hucaby, Cisco ASA and PIX Firewall Logging, last modified: November 4, 2005, http://www.ciscopress.com/articles/article.asp?p=424447&seqNum=2.
1749. Cisco ASA 5500 Series Command Reference, 8.2, https://www.cisco.com/c/en/us/td/docs/security/asa/asa82/command/reference/cmd_ref/cli.html.
1750. Identifying Incidents Using Firewall and Cisco IOS Router Syslog Events, https://www.cisco.com/c/en/us/about/security-center/identify-incidents-via-syslog.html.
1751. Next Generation Firewall, https://www.checkpoint.com/products/next-generation-firewall/.
1752. Check Point Firewall Security Solution, last modified: 2013, https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/html_frameset.htm.
1753. Introduction to the Command Line Interface, https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm.

1754. Configure logging in Cisco IOS, last modified: December 10, 2013, https://blog.router-switch.com/2013/12/configure-logging-in-cisco-ios/.
1755. How to configure logging in Cisco IOS, last modified: August 23, 2017, https://community.cisco.com/t5/networking-documents/how-to-configure-logging-in-cisco-ios/ta-p/3132434.
1756. Router log analysis, https://www.manageengine.com/products/eventlog/monitor-router-logs.html.
1757. System Message Logging, last modified: March 11, 2008, https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html.
1758. System Message Logging, last modified: 2009, https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.pdf.
1759. Cisco IOS Configuration Fundamentals Command Reference, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.pdf.
1760. Cisco & Cisco Network Hardware News and Technology, last modified: December 11, 2013, http://ciscorouterswitch.over-blog.com/article-show-logging-121540379.html.
1761. Matt Watson, Where Are IIS Log Files Located? How to View IIS Logs on Windows & Azure, last modified: April 7, 2017, https://stackify.com/where-are-iis-log-files-located/.
1762. Nicholas J, What Are IIS Log Files?, https://www.techwalla.com/articles/what-are-iis-log-files.
1763. IIS Log File Formats, last modified: June 16, 2017, https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms525807(v=vs.90).
1764. Brena Monteiro, Understanding and Analyzing IIS Logs, last modified: July 31, 2017, https://www.sumologic.com/blog/using-sumo/iis-logs/.
1765. W3C Logginglast modified: May 31, 2018, https://docs.microsoft.com/en-us/windows/desktop/http/w3c-logging.
1766. Guidelines Detecting Signs of Intrusion V103, last modified: April 05, 2018, https://vdocuments.us/guidelines-detecting-signs-of-intrusion-v103.html?h=vdocuments.com.br.
1767. Logging and Monitoring, https://www.feistyduck.com/library/apache-security/online/apachesc-CHP-8.html.
1768. Log Files, https://httpd.apache.org/docs/2.4/logs.html.
1769. Jason Skowronski, Apache Logging Basics Log Files, last modified: 2017, https://www.loggly.com/ultimate-guide/apache-logging-basics/.
1770. Apache Logs Viewer Manual, https://www.apacheviewer.com/doc/ALVHelp.pdf.
1771. Vivek Gite, Apache Log Files, last modified: June 08, 2008, https://www.cyberciti.biz/faq/apache-logs/.
1772. How to view Apache log files,https://www.a2hosting.in/kb/developer-corner/apache-web-server/viewing-apache-log-files.
1773. Understanding the Apache Access Log, last modified: October 04, 2018, https://www.keycdn.com/support/apache-access-log.
1774. Brena Monteiro, Working with Apache Error Log Files, last modified: July 31, 2017, https://www.sumologic.com/blog/using-sumo/apache-error-logs/.
1775. Blane Warrene, Configure Web Logs in Apache, last modified: February 23, 2004, https://www.sitepoint.com/configuring-web-logs-apache/.
1776. Jamie Morgan, What is Centralized Log Management (CLM)?, last modified: May 31, 2016, https://www.missioncloud.com/blog/what-is-centralized-log-management-clm/.
1777. MSS - TS: Types of Log Collection Methods, last modified: July 14th, 2017, https://support.symantec.com/en_US/article.INFO4456.html.
1778. Log Collection: The Basics, last modified: May 4, 2017, https://community.rsa.com/docs/DOC-42977.
1779. Rajesh K, An Overview of Syslog and Syslog Server, last modified: July 27, 2009, http://www.excitingip.com/421/an-overview-of-syslog-and-syslog-server/.
1780. R. Gerhards, The Syslog Protocol, last modified: March 2009, https://tools.ietf.org/html/rfc5424.
1781. What is Syslog?, last modified: May 24, 2017, https://blog.rapid7.com/2017/05/24/what-is-syslog/.
1782. Syslog Tutorial: How It Works, Examples, Best Practices, and More, last modified: June 30, 2017, https://stackify.com/syslog-101/.
1783. Radu Gheorghe, What is Syslog: Daemons, Message Formats and Protocols, last modified: January 30, 2017, https://sematext.com/blog/what-is-syslog-daemons-message-formats-and-protocols/.
1784. What is Syslog?, https://www.paessler.com/it-explained/syslog.
1785. syslog-ng Open Source Edition 3.16 - Administration Guide, https://syslog-ng.com/documents/html/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/concepts-message-bsdsyslog.html.
1786. R. Gerhards, Syslog Message Format, last modified: March 2009, https://tools.ietf.org/html/rfc5424#section-6.
1787. Jason Wilder, Centralized Logging Architecture, last modified: July 16, 2013, http://jasonwilder.com/blog/2013/07/16/centralized-logging-architecture/.
1788. Adrian Lane, Understanding and Selecting SIEM/LM: Aggregation, Normalization, and Enrichment, last modified: May 27, 2010, https://securosis.com/blog/understanding-and-selecting-siem-lm-aggregation-normalization-and-enrichmen.
1789. Event normalization in SIEM, https://vpotapov.wordpress.com/2017/02/13/event-normalization/.
1790. Alex Teixeira, Get over SIEM event normalization, last modified: November 08, 2017, https://medium.com/@ateixei/get-over-siem-event-normalization-595fc36559b4.
1791. Dr. Anton Chuvakin, The Complete Guide to Log and Event Management, last modified: March 2010, https://www.novell.com/docrep/documents/9x1wixnqhd/Log_Event_Mgmt_WP_DrAntonChuvakin_March2010_Single_en.pdf.
1792. Javvad Malik, What is Event Log Correlation?, last modified: February 8, 2019, https://www.alienvault.com/resource-center/videos/what-is-event-log-correlation.
1793. Log Analysis, https://www.techopedia.com/definition/31756/log-analysis.

1794. Ellen Zhang, What is Log Analysis? Use Cases, Best Practices, and More, last modified: September 12, 2018, https://digitalguardian.com/blog/what-log-analysis-use-cases-best-practices-and-more.

1795. Kathleen Estreich, Erik Dietrich, What Goes Into Log Analysis?, last modified: December 31, 2017, https://dzone.com/articles/what-goes-into-log-analysis.

1796. Twain Taylor, Machine Learning and Log Analysis, last modified: July 31, 2017, https://www.sumologic.com/blog/using-sumo/machine-learning-log-analysis/.

1797. Matt Kiernan, 10 Best Practices for Log Management and Analytics, last modified: January 21, 2016, https://dzone.com/articles/10-best-practices-for-log-management-and-analytics-1.

1798. Syslog Alerting, last modified: August 03, 2016, https://docs.observium.org/alerting_syslog/.

1799. Liron Tal, 9 Logging Best Practices Based on Hands-on Experience, last modified: January 25, 2017, https://www.loomsystems.com/blog/single-post/2017/01/26/9-logging-best-practices-based-on-hands-on-experience.

1800. Mr Neil Robinson, Ms. Veronika Horvath, Prof Jonathan Cave, Dr Arnold P. Roosendaal, Dr Marieke Klaver, Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts, last modified: September 2013, http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf.

1801. Security Incident, https://www.techopedia.com/definition/15957/security-incident.

1802. Margaret Rouse, security Incident, last modified: November 2016, https://whatis.techtarget.com/definition/security-incident.

1803. John Spacey, Security Event Vs Security Incident, last modified: November 16, 2016, https://simplicable.com/new/security-event-vs-security-incident.

1804. Daniel Miessler, The Difference Between Events, Alerts, and Incidents, last modified: November 15, 2017, https://danielmiessler.com/study/event-alert-incident/.

1805. Log file, last modified: December 31, 2018, https://en.wikipedia.org/wiki/Log_file.

1806. Ivy Wigmore, Margaret Rouse, log (log file), last modified: November 2014, https://whatis.techtarget.com/definition/log-log-file.

1807. Conard Constantine, What kind of logs do you need for an effective SIEM implementation?, last modified: March 18, 2014, https://www.alienvault.com/blogs/security-essentials/what-kind-of-logs-for-effective-siem-implementation.

1808. Matt Stevens, Security Information and Event Management (SIEM), last modified: October 08, 2005, https://www.certconf.org/presentations/2005/files/WC4.pdf.

1809. Everything You Always Wanted to Know About Log Management but Were Afraid to Ask, last modified: August 21, 2103, http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/Log%20Management.pdf.

1810. Business Case for Security Analytics, http://www.ecominfotech.biz/SOC.html.

1811. Security Log, last modified: 2012, https://www.webnms.com/cagent/help/tl1/c_tl1_seculog.html.

1812. Vivek Gite, Linux Log Files Location And How Do I View Logs Files on Linux?, last modified: December 6, 2014, https://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/.

1813. Roger A. Grimes, Why you need centralized logging and event log management, last modified: June 12, 2018, https://www.csoonline.com/article/3280123/data-breach/why-you-need-centralized-logging-and-event-log-management.html.

1814. Log Management and Visibility for Modern Applications, https://www.scalyr.com/product/centralized-log-management.

1815. Chris Petersen, Log and event management appliances improve compliance, security, operations, last modified: March 19, 2008, https://www.networkworld.com/article/2284650/tech-primers/log-and-event-management-appliances-improve-compliance--security--operations.html.

1816. Security Information and Event Management (SIEM), last modified: March 07, 2014, https://www.slideshare.net/k33a/security-information-and-event-management-siem.

1817. What is the difference between syslog, rsyslog and syslog-ng?, last modified: July 2018, https://serverfault.com/questions/692309/what-is-the-difference-between-syslog-rsyslog-and-syslog-ng.

1818. Angela Stringfellow , Log Aggregation 101: Methods, Tools, Tutorials and More, last modified: September 30, 2017, https://stackify.com/log-aggregation-101/.

1819. syslog-ng Open Source Edition 3.16 - Administration Guide, https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.16/administration-guide#TOPIC-956384.

1820. Eran Cohen, How Security Operations Can Safely Stop Investigating Benign True Positives, last modified: April 20, 2017, https://blog.preempt.com/how-security-operations-can-safely-stop-investigating-benign-true-positives.

1821. Amarnath G, what is false positive, false negetive, true positive and true negetive?, last modified: April 25, 2015, https://community.softwaregrp.com/t5/ArcSight-User-Discussions/what-is-false-positive-false-negetive-true-positive-and-true/td-p/1582039.

1822. Glenn Cater, Hal Tipton, Micki Krause, Security Event Management, last modified: 2009, http://www.infosectoday.com/Articles/Security_Event_Management/Security_Event_Management.htm

1823. Afsaneh Madani, Saed Rezayi, Hossein Gharaee, Log management comprehensive architecture in Security Operation Center (SOC), last modified: 2011, https://www.semanticscholar.org/paper/Log-management-comprehensive-architecture-in-Center-Madani-Rezayi/a4078c7f56fb96e8feb26c56c9c880167422d447.

1824. Endpoint Security-Using Artificial Intelligence and Machine Learning, from https://www.vlcsolutions.com/blog/endpoint-security-using-artificial-intelligence-and-machine-learning/.

1825. How Artificial Intelligence (AI) and Machine Learning(ML) Transforming Endpoint Security, from https://www.geeksforgeeks.org/how-artificial-intelligence-ai-and-machine-learningml-transforming-endpoint-security/.

1826. Pradeep Makhija (06 Jul 2020), 6 Ways AI and ML Together Transforming Endpoint security in 2020, from https://www.techiexpert.com/6-ways-ai-and-ml-together-transforming-endpoint-security-in-2020/.

1827. 24 Aug 2023, Network monitoring, from https://www.linkedin.com/advice/1/how-can-you-use-ai-improve-network-performance#:~:text=AI%20can%20enhance%20network%20monitoring,failures%2C%20and%20prioritize%20network%20issues.

1828. 19 July 2022, Behavioral Analysis and AI/ML for Threat Detection, from https://www.proofpoint.com/us/blog/email-and-cloud-threats/behavioral-analysis-and-aiml-threat-detection-going-behind-scenes.

1829. John Herrema (27 may 2021), The BlackBerry Approach to Network Threat Modeling, from https://blogs.blackberry.com/en/2021/05/the-role-of-artificial-intelligence-and-machine-learning-in-threat-detection#:~:text=The%20BlackBerry%20approach%20to%20network%20threat%20modeling%20is%20based%20on,%2C%20and%20malware%2FC2%20detection.

Module 16 Incident Response and Forensic Investigation

1830. Incident Response Planning Guideline, from https://security.berkeley.edu/incident-response-planning-guideline.

1831. Responding to IT Security Incidents, from https://technet.microsoft.com/en-us/library/cc700825.aspx.

1832. Chris Cox, The network administrator's guide to forensic first response, from http://searchnetworking.techtarget.com/tip/The-network-administrators-guide-to-forensic-first-response.

1833. malicious code, from http://www.webopedia.com/TERM/M/malicious_code.html.

1834. Unauthorized access, from http://www.computerhope.com/jargon/u/unauacce.htm.

1835. Unauthorized Use of Resources, from http://web.physics.ucsb.edu/~pcs/policies/hacking.html.

1836. Computer Fraud from http://www.computerhope.com/jargon/c/computer-fraud.htm.

1837. Theft, from http://www.computerhope.com/jargon/t/theft.htm.

1838. Information Security Incident Identification, from https://about.usps.com/handbooks/as805/as805c13_002.htm.

1839. Examples of Security Incidents, from http://www.bu.edu/tech/services/security/cyber-security/sensitive-data/reporting/examples/.

1840. Adli Wahid (May 2014), Incident Response & Handling, from https://nsrc.org/workshops/2014/bdnog1/raw-attachment/wiki/Track2Agenda/4.CSIRT-Module.pdf.

1841. NIST(Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang), Guide to Integrating Forensic Techniques into Incident Response, from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

1842. Bruce J. Nikkel (September 2, 2005), Generalizing sources of live network evidence, from http://www.digitalforensics.ch/ nikkel05a.pdf.

1843. Network Forensics, from http://www.techopedia.com/definition/16122/network-forensics.

1844. Network Forensics,http:// www.cyberforensics.in/(A(3g36EzYuzQEkAAAAMGJjNmZmNDctODliNy00NTFkLWFhYTktNGRmMGVmMzhmOTYz78nqDBqkizzKAWLXIBU8H9tUYR81))/Research/NetworkForensics.aspx?AspxAutoDetectCookieSupport=1.

1845. Network forensics , from http://en.wikipedia.org/wiki/Network_forensics.

1846. John Ashcroft (Attorney General), Deborah J. Daniels (Assistant Attorney General), Sarah V. Hart (Director Institute of Justice), Forensic Examination of Digital Evidence A Guide for Law Enforcement, from https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

1847. Chris Cox, The network administrator's guide to forensic first response, from http://searchnetworking.techtarget.com/tip/The-network-administrators-guide-to-forensic-first-response.

1848. WHAT DOES AN INCIDENT RESPONDER DO? , from http://www.cyberdegrees.org/jobs/incident-responder/

1849. Richard Nolan, Colin O'Sullivan, Jake Branson, Cal Waits(March 2005), First Responders Guide to Computer Forensics, from http://www.sei.cmu.edu/reports/05hb001.pdf.

1850. NIST (Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone), Computer Security Incident Handling Guide from http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

1851. Machine learning enhances threat detection, from https://expel.com/blog/the-role-of-artificial-intelligence-in-threat-hunting/#:~:text=Machine%20learning%20algorithms%20also%20teach,alerts%20within%20your%20security%20tools.

1852. What are some of the innovative ways that incident handlers use artificial intelligence and machine learning, from https://www.linkedin.com/advice/0/what-some-innovative-ways-incident-handlers-use.

1853. Threat Modeling AI/ML Systems and Dependencies, from https://learn.microsoft.com/en-us/security/engineering/threat-modeling-aiml.

1854. Jonathan Reed (21 Jun 2023), AI assistance cuts alert triage times in half, from https://securityintelligence.com/news/ai-assistance-cuts-alert-triage-times-in-half/.

1855. Andrew Mairena (17 Jan 2020), How AI finally learned to triage IT support issues, from https://www.moveworks.com/insights/how-ai-triages-it-support-issues-part-2.

1856. How do you leverage artificial intelligence or machine learning for incident handling, from https://www.linkedin.com/advice/0/how-do-you-leverage-artificial-intelligence-machine-1c.

1857. Incident response automation: What it is and how it works, from https://www.techtarget.com/searchsecurity/tip/Incident-response-automation-What-it-is-and-how-it-works#:~:text=What%20is%20incident%20response%20automation,threaten%20an%20organization's%20cybersecurity%3B%20and.

1858. AI in Cybersecurity: Incident Response Automation Opportunities, from https://www.sisainfosec.com/blogs/ai-in-cybersecurity-incident-response-automation-opportunities/.

1859. Mark (07 Jul 2023), The Impact of Machine Learning on Cybersecurity Incident Response, from https://www.markaicode.com/the-impact-of-machine-learning-on-cybersecurity-incident-response/.

1860. Anthony M. Freed, AI-Driven XDR: Defeating the Most Complex Attack Sequences, from https://www.cybereason.com/blog/ai-driven-xdr-defeating-the-most-complex-attack-sequences#:~:text=What%20is%20an%20AI%2Ddriven,%2C%20applications%2C%20and%20the%20network.

1861. How SIEM with AI/ML is Revolutionizing the SOC, from https://www.exabeam.com/explainers/siem/ai-siem-how-siem-with-ai-ml-is-revolutionizing-the-soc/#:~:text=Automated%20Incident%20Response&text=AI%2Dbased%20SIEM%20employs%20options,even%20orchestrate%20complex%20response%20workflows.

1862. What is UEBA (user and entity behavior analytics), from https://www.ibm.com/topics/ueba.

1863. Bill Doerrfeld (31 May 2023), How AI Enhances Endpoint Detection and Response (EDR) for Stronger Cybersecurity, from https://accelerationeconomy.com/cybersecurity/how-ai-enhances-endpoint-detection-and-response-edr-for-stronger-cybersecurity/.

1864. Mike Costello, 11 EDR Key Features Your Enterprise Solution Should Have, from https://solutionsreview.com/endpoint-security/edr-key-features-your-enterprise-solution-should-have/.

1865. Nolan Foster (01 Jul 2022), 7 Benefits of EDR(Endpoint Detection and Response) for Your Organization, from https://www.acecloudhosting.com/blog/7-benefits-of-edr/.

1866. Malware detection, from https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/index.html?highlight=malware%20detection.

1867. Umut Arslanoglu (21 May 2023), What is Endpoint Detection and Response, from https://www.xcitium.com/edr-security/edr-endpoint-detection-and-response/.

1868. What are EDR (Endpoint Detection and Response) Solutions, from https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions.

1869. SolarWinds Remote Monitoring and Management Integrates SolarWinds Endpoint Detection and Response Capabilities, from https://investors.solarwinds.com/news/news-details/2020/SolarWinds-Remote-Monitoring-and-Management-Integrates-SolarWinds-Endpoint-Detection-and-Response-Capabilities/default.aspx.

1870. Comprehensive Cybersecurity Made Easy, from https://www.cynet.com/.

1871. The Importance of EDR Security, from https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-endpoint-detection-and-response/#:~:text=Remediation%20Automation%3A%20EDR%20solutions%20can,reduces%20load%20on%20security%20analysts.

1872. Gavin Wright, Endpoint detection and response (EDR), from https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR.

1873. How Endpoint Detection and Response Works, from https://www.blackberry.com/us/en/solutions/endpoint-security/endpoint-detection-and-response/how-edr-works.

1874. Pramod Borkar (02 May 2023), Incident Response, from https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/.

1875. Discover the AI-native CrowdStrike Falcon XDR platform, from https://www.crowdstrike.com/falcon-platform/?utm_campaign=brand&utm_content=crwd-treq-en-x-tct-ind-psp-x-trl-brnd-x_x_x_x-product&utm_medium=sem&utm_source=goog&utm_term=crowdstrike%20falcon&cq_cmp=19634319550&cq_plac=&gad=1&gclid=EAIaIQobChMIoaG0xKXhgQMV9aRmAh017w1xEAAYAiAAEgLm0PD_BwE.

1876. Endpoint Security, from https://www.broadcom.com/products/cybersecurity/endpoint#endpoint-security.

1877. What Is Extended Detection and Response (XDR), from https://www.paloaltonetworks.com/cyberpedia/what-is-xdr.

1878. What Is XDR, from https://www.trellix.com/en-in/security-awareness/endpoint/what-is-xdr.html.

1879. Anne Aarness (18 April 2023), XDR Definition, from https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/.

1880. Michael Sentonas (10 Feb 2022), Extending Detection and Response , from https://www.crowdstrike.com/blog/how-falcon-xdr-extends-detection-and-response-the-right-way/.

1881. Experience cybersecurity like never before with SIEM, from https://www.manageengine.com/log-management/?pos=Log360&loc=ProdMenu&cat=SIEM.

1882. Best Extended Detection and Response (XDR) Platforms for Enterprise Businesses, from https://www.g2.com/categories/extended-detection-and-response-xdr-platforms/enterprise.

1883. Sam Ingallas (19 May 2023), Top 10 XDR (Extended Detection & Response) Security Solutions, from https://www.esecurityplanet.com/products/xdr-security-solutions/.

1884. 10 Best XDR Solutions: Extended Detection And Response Services In 2023, from https://www.softwaretestinghelp.com/xdr-security-solutions/.

1885. Ben Filipkowski (11 Jul 2023), What is the difference between MDR, XDR, and EDR, from https://fieldeffect.com/blog/mdr-xdr-edr.

1886. Ron Samson (11 Aug 2022), MDR Vs EDR Vs XDR: What's Best For Your Business, from https://www.clearnetwork.com/mdr-vs-edr/.

1887. Nick Hayes (18 Apr 2023), EDR VS MDR VS XDR, from https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/.

1888. What is Cybersecurity Analytics, from https://www.fortinet.com/resources/cyberglossary/cybersecurity-analytics.

1889. What is Data Integration - Popular Methods And Applications, from https://www.simplilearn.com/what-is-data-integration-article.

1890. What is SOAR, from https://www.ibm.com/topics/security-orchestration-automation-response.

1891. How does SOAR work, from https://www.microsoft.com/en-in/security/business/security-101/what-is-soar#:~:text=SOAR%20is%20typically%20composed%20of,accessed%20from%20one%20central%20place.

1892. Sharon Shea, SOAR (security orchestration, automation and response), from https://www.techtarget.com/searchsecurity/definition/SOAR.
1893. What is SOAR? Functional Components & Benefits, from https://www.newevol.io/resources/blog/orchastration-response/what-is-soar/.
1894. SOAR (Security, Orchestration, Automation, and Response), from https://www.fortinet.com/resources/cyberglossary/what-is-soar.
1895. Dario Forte (31 Jul 2020), Five critical Components of SOAR, from https://www.sumologic.com/blog/five-critical-components-of-soar-technology/.
1896. What is a Cybersecurity Response Playbook, from https://cofense.com/knowledge-center/what-is-a-cyber-response-playbook/#:~:text=A%20cyber%20security%20response%20playbook%20is%20a%20plan%20that%20outlines,incidents%20with%20cyber%20response%20playbooks.
1897. SOAR Security: How It Works, Use Cases, and Key Features, from https://www.bluevoyant.com/knowledge-center/soar-security-how-it-works-use-cases-and-key-features.
1898. What are Security Orchestration, Automation and Response Solutions, from https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions.
1899. SOAR Security, from https://www.checkpoint.com/cyber-hub/threat-prevention/soar-security-what-is-security-orchestration-automation-and-response/.
1900. SOAR (Security Orchestration Automation and Response) Definition, Best Practices and Tools, from https://medium.com/@cloud_tips/soar-security-orchestration-automation-and-response-definition-best-practices-and-tools-8a20dd590bd5.
1901. Splunk SOAR Features, from https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation-features.html.
1902. Chrissy Kidd (06 Dec 2023), SOAR: Security Orchestration, Automation & Response, from https://www.splunk.com/en_us/data-insider/what-is-soar.html.
1903. Threat detection, from https://www.manageengine.com/log-management/features.html.
1904. Security Incident Response (SIR), from https://www.servicenow.com/products/security-incident-response.html.
1905. Security Incident Response, from https://docs.servicenow.com/bundle/vancouver-security-management/page/product/security-incident-response/reference/sir-landing-page.html.
1906. Threat-hunting & Action Center, from https://heimdalsecurity.com/enterprise-security/products/threat-hunting-action-center.
1907. IBM Security QRadar SOAR, from https://www.ibm.com/products/qradar-soar.
1908. AI Enabled Automation for the Entire Security Organization, from https://swimlane.com/.
1909. Security Orchestration, Automation and Response (SOAR) Capabilities, from https://swimlane.com/assets/uploads/documents/SOAR_Capabilities_e_book___Swimlane.pdf.
1910. Break Product Silos to Automate Incident Response, from https://apps.paloaltonetworks.com/marketplace/demisto.

Module 17 Business Continuity and Disaster Recovery

1911. Continuity Central, what is business continuity? From https://www.continuitycentral.com/index.php/businesscontinuity
1912. MTSFB (October 15, 2018) Business Continuity Management (BCM) - Requirements, from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-MTSFB-TC-G014_2018_BUSINESS-CONTINUITY-MANAGEMENT-(BCM)-REQUIREMENTS.pdf
1913. M.el Khamlichi (October 9, 2015) What is Disaster Recovery? from https://www.unixmen.com/what-is-disaster-recovery/
1914. ITcentric (June 14, 2017) How to disaster plan for business continuity, from https://itcentric.co.uk/the-importance-of-a-robust-disaster-recovery-plan/
1915. Will Kenton (June 1, 2019) Business Continuity Planning (BCP), from https://www.investopedia.com/terms/b/business-continuity-planning.asp
1916. Michael Herrera (July 13, 2017) 10 Benefits Of Business Continuity Planning, from https://bcmmetrics.com/benefits-business-continuity-planning/
1917. Techopedia (May 23, 2012) Contingency Plan, from https://www.techopedia.com/definition/13595/contingency-plan
1918. RockDove Solutions, 3 Differences Between Emergency Preparedness and Business Continuity, from https://www.rockdovesolutions.com/blog/3-differences-between-emergency-preparedness-and-business-continuity
1919. Philip P. Purpura (2008) Security and Loss Prevention (Fifth Edition), from https://www.rockdovesolutions.com/blog/3-differences-between-emergency-preparedness-and-business-continuity
1920. IBM Services (July 3, 2019) Adapt and respond to risks with a business continuity plan (BCP), from https://www.ibm.com/services/business-continuity/plan
1921. IT Service Management Office, Business Impact Analysis (BIA), from http://itsm.ucsf.edu/business-impact-analysis-bia-0
1922. Ready (December 11, 2015) Business Impact Analysis, from https://www.ready.gov/business-impact-analysis
1923. Martin Luenendonk (March 21, 2017) How to Perform a Business Impact Analysis, from https://www.cleverism.com/business-impact-analysis/
1924. NHS Information Authority (May 2003) Business Continuity Planning, from https://www.igt.hscic.gov.uk/Knowledgebase/Kb/Business%20Continuity%20Management/businesscontinuitymanual.pdf.
1925. Paul Kirvan, Business resilience, from https://www.techtarget.com/searchcio/definition/business-resilience.
1926. Strategies for building business resilience, from https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-business-resilience.html#~strategies.

1927. Organizational resilience, from https://www.ckju.net/en/dossier/organizational-resilience-what-it-and-why-does-it-matter-during-a-crisis.
1928. Tools & resources for measuring organisational resilience, from https://www.resorgs.org.nz/about-resorgs/what-is-organisational-resilience/.
1929. Operational Resilience, from https://www.gartner.com/en/information-technology/glossary/operational-resilience.
1930. What is cyber resilience, from https://www.ibm.com/topics/cyber-resilience.
1931. Supply chain resiliency in detail, from https://www.sap.com/products/scm/integrated-business-planning/what-is-a-resilient-supply-chain.html.
1932. A Complete Guide to Business Continuity Management, from https://standard.com/en-sg/blog/business-continuity-management/.
1933. What is Emergency Management, from https://www.maine.gov/mema/about/emergency-management#:~:text=Emergency%20management%20protects%20communities%20by,or%20other%20man%2Dmade%20disasters.
1934. John Leo Weber (24 Jun 2022), What Is Business Impact Analysis & Why Is It Important, from https://www.projectmanager.com/blog/business-impact-analysis.
1935. Cybersecurity Risk Management, from https://www.imperva.com/learn/data-security/cybersecurity-risk-management/.
1936. Step-by-Step Guide to Writing a Crisis Management Plan, from https://www.smartsheet.com/content/crisis-management-plan.
1937. Crisis Management Plan: Definition, Types & Steps to Create, from https://blog.bit.ai/crisis-management-plan/.
1938. Crisis Management Plan, rom https://www.managementstudyguide.com/crisis-management-plan.htm.
1939. Crisis Management - Meaning, Need and its Features, from https://www.managementstudyguide.com/crisis-management.htm.
1940. Andrew Gorecki (16 Jul 2020), Deciphering Between Incident Management and Crisis Management, from https://securityintelligence.com/posts/benefits-differences-incident-crisis-management/.
1941. Andy Marker (15 Jun 2020), Step-by-Step Guide to Writing a Crisis Management Plan, from https://www.smartsheet.com/content/crisis-management-plan.
1942. Khaled Ismail, The Key Elements of a Crisis Management Plan, from https://hsseworld.com/the-key-elements-of-a-crisis-management-plan/#The_Key_Elements_of_a_Crisis_Management_Plan.
1943. 20 May 2020, How to Create a Cybersecurity Crisis Management Plan in 5 Steps, from https://www.getapp.com/resources/cybersecurity-crisis-management-plan/.
1944. Crisis Management Plan, from https://www.techno-pm.com/2021/09/crisis-management-plan.html.
1945. Major Factors to Consider in Crisis Management Planning, from https://www.noggin.io/blog/major-factors-to-consider-in-crisis-management-planning.
1946. Yahya Maresh (15 Feb 2021), Factors Influencing Crisis Management, from https://www.tandfonline.com/doi/full/10.1080/23311975.2021.1878979.
1947. 30 Nov 2020, What is a crisis management plan, from https://asana.com/resources/crisis-management-plan.
1948. Cyber Security Risk Assessments, from https://www.itgovernance.asia/cyber-security-risk-assessments-10-steps-to-cyber-security#:~:text=A%20cyber%20security%20risk%20assessment%20is%20the%20process%20of%20identifying,waste%20time%2C%20effort%20and%20resources.
1949. What is a Cyber Security Risk Assessment, from https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-cyber-security-risk-assessment/.
1950. Five Ways to Minimize Risk Exposure, from https://www.optiv.com/explore-optiv-insights/blog/five-ways-minimize-risk-exposure.
1951. Security Risk Assessment, from https://www.synopsys.com/glossary/what-is-security-risk-assessment.html.
1952. Crisis Communication: Definition, Importance and Best Practices, from https://haiilo.com/blog/crisis-communication-definition-importance-best-bractices/.
1953. Cyber Risk Prioritization, from https://reciprocity.com/blog/how-to-prioritize-cyber-risk-for-your-organization/.
1954. 12 Jul 2021, Understanding the Differences between Incident Response, Disaster Recovery, and Business Continuity, from https://www.goldskysecurity.com/understanding-the-differences-between-incident-response-disaster-recovery-and-business-continuity/.
1955. DIFFERENCE BETWEEN DR, BC AND CRISIS MANAGEMENT (CM), from https://www.stayinbusiness.com/difference-between-dr-bc-and-crisis-management-cm/.
1956. What is a Disaster Recovery Plan, from https://cloud.google.com/learn/what-is-disaster-recovery#:~:text=IT%20disaster%20recovery%20is%20a,disaster%20recovery%20plan%20is%20cloud.
1957. Adam Hayes (22 Mar 2022), Crisis Management: Definition, How It Works, Types, and Example, from https://www.stayinbusiness.com/difference-between-dr-bc-and-crisis-management-cm/#:~:text=Business%20continuity,-This%20aspect%20of&text=Crisis%20Management%20Plan%2C%20DR%20and,taken%20to%20handle%20the%20crisis.
1958. Why integrate BC, risk management, and crisis management, from https://www.linkedin.com/advice/0/how-do-you-integrate-your-bc-plan-risk-management#:~:text=Integrating%20BC%2C%20risk%20management%2C%20and,making%20and%20communication%20during%20emergencies.
1959. Crisis management and business continuity planning, from https://www.infoentrepreneurs.org/en/guides/crisis-management-and-business-continuity-planning/.
1960. Chantal (03 Nov 2020), Integrating Crisis Management & Business Continuity for a successful response, from https://www.thebci.org/news/integrating-crisis-management-business-continuity-for-a-successful-response.html.
1961. 7 Steps to a Successful Disaster Recovery Plan, from https://www.lightedge.com/blog/7-steps-to-a-successful-disaster-recovery-plan/.
1962. 10 Key Elements of a Disaster Recovery Plan, from https://blog.opti9tech.com/10-key-elements-of-a-disaster-recovery-plan.

1963. Booby Guerra (19 Jun 2023), Components That Make A Great Disaster Recovery Plan, from https://www.axiom.tech/7-components-that-make-a-great-disaster-recovery-plan/.

1964. Business continuity planning (BCP), from https://www.imperva.com/learn/availability/business-continuity-planning/.

1965. The 10 Components of a Business Continuity Plan, from https://www.xometry.com/resources/shop-tips/the-10-components-of-a-business-continuity-plan/.

1966. What are the key components of a business continuity plan, from https://www.linkedin.com/advice/0/what-key-components-business-continuity-plan.

1967. What is Risk Mitigation, from https://reciprocity.com/resources/what-is-risk-mitigation/.

1968. John Moore, what is BCDR? Business continuity and disaster recovery guide, from https://www.techtarget.com/searchdisasterrecovery/definition/Business-Continuity-and-Disaster-Recovery-BCDR#:~:text=The%20role%20of%20BCDR%20is,decreasing%20the%20chance%20of%20emergencies.

1969. Dejan Kosutic, Information security & business continuity standards, from https://advisera.com/27001academy/knowledgebase/information-security-business-continuity-standards/.

1970. BUSINESS CONTINUITY STANDARDS & FRAMEWORKS, from https://www.stayinbusiness.com/business-continuity-standards-frameworks/.

1971. Standard for Emergency, Continuity, and Crisis Management: Preparedness, Response, and Recovery, from https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1660.

1972. Marianne Swanson (17 Mar 2023), Contingency Planning Guide for Federal Information Systems, from https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final.

1973. Risk management, from https://www.iso.org/standard/44651.html.

Module 18 Risk Anticipation with Risk Management

1974. Enterprise Risk Management Framework 2012–2016, from http://deta.qld.gov.au/corporate/pdf/enterprise-risk-management-framework.pdf.

1975. Treating risks, from http://www.business.qld.gov.au/business/starting/starting-a-business/managing-risk/treating-risks.

1976. Risk Treatment, from http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment.

1977. Luiz Renato Lima, Breno Pinheiro N´eri, Comparing Value-at-Risk Methodologies, from http://bibliotecadigital.fgv.br/ojs/index.php/bre/article/viewFile/1570/1010.

1978. Treat risks to your business, from http://www.business.qld.gov.au/business/running/risk-management/risk-management-plan-business-impact-analysis/treat-risks-business.

1979. February 2008, AN OVERVIEW OF VULNERABILITY SCANNERS, from http://www.infosec.gov.hk/ english/technical/files/vulnerability.pdf.

1980. September 2004, Enterprise Risk Management —Integrated Framework Executive Summary, from http://www.coso.org/publications/erm/coso_erm_executivesummary.pdf.

1981. SEPTEMBER 1, 2004, Why Has COSO Prepared this ERM Framework, from http://erm.ncsu.edu/library/article/coso-erm-framework#.U_biLsWSwYw.

1982. What is COBIT5, from http://www.isaca.org/COBIT/Pages/default.aspx.

1983. Michael Gibson March 1997, Information systems for risk management, from http://www.bis.org/publ/ecsc07f.pdf.

1984. Risk management information systems, from http://en.wikipedia.org/wiki/Risk_Management_Information_Systems.

1985. May 23, 2013, What is a risk management information system & what can it do for you? from http://blog.aon-esolutions.com/blog/bid/286243/What-is-a-risk-management-information-system-what-can-it-do-for-you.

1986. RMIS: Taking Data Management Enterprisewide, from http://cf.rims.org/Magazine/PrintTemplate.cfm?AID=2899.

1987. Risk Management Information System The Definitive Guide to a Risk Management Information System, from http://www.aon.com/netherlands/risk-console/documents/Aon-RMIS-RiskConsole-Brochure.pdf .

1988. Risk Management lnformation Systems (RMIS) , from http:// www.mapfre.com/ documentacion/publico/i18n/catalogo_imagenes/grupo.cmd?path=1065767.

1989. Aon Enterprise Risk Management, from http://www.aon.com/risk-services/enterprise-risk-mgmt.jsp.

1990. RiskEnvision, from http://www.ebix.com/Contents/risk_envision.

1991. Risk Management Information Systems, from http://riskonnect.com/risk-management-information-systems.

1992. Inform Reporting Tool System Overview, from http://www.informapplications.com/index-4.html.

1993. Risk Management Information Services (RMIS), from https://www.travelers.com/business-insurance/large-business/risk-management-information-services/index.aspx.

1994. Insight ERM Services, from http://insightrisktech.com/insight-erm-services/ .

1995. Enterprise Security Policy, from http://www.its.ms.gov/Services/Pages/ENTERPRISE-SECURITY-POLICY.aspx.

1996. Shon Harris, How to write an information risk management policy, from http://searchsecurity.techtarget.com/tip/How-to-write-an-information-risk-management-policy.

1997. Privacy Policy, from http://reboottwice.com/privacy-policy/.

1998. Risk Management Policy, from http://www.usg.edu/policymanual/section7/policy/C1504.

1999. Phil McNaull / Lorraine Loy (Dec 208), RISK MANAGEMENT, from http://www1.hw.ac.uk/insurance/risk-management-policy.pdf.

References

2000. Risk Management Policy D09/1896P, from http://www.newcastle.edu.au/policy/000601.html.

2001. CSU Policy Library , from www.csu.edu.au/adminman/gov/policy-risk-management.pdf.

2002. BUSINESS CONTINUITY PLANNING (BCP), from http://www.sjsu.edu/adminfinance/docs/BCP_Master_Plan.pdf.

2003. 2010, Top Ten 'Next' Practices for Enterprise Risk Management, from http://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/erm_next_practices_report.pdf.

2004. 7 steps to effective risk management, from http://www.networkworld.com/newsletters/ 2008/052608itlead1.html.

2005. Vulnerability management , from https://en.wikipedia.org/wiki/Vulnerability_management.

2006. Vulnerability Management, from http://www.veracode.co.uk/security/vulnerability-management.

2007. https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management.

2008. Amrit T. Williams, Mark Nicolett (02 May 2005), from Improve IT Security With Vulnerability Management http://searchsecurity.techtarget.com/magazineContent/Framework-for-building-a-vulnerability-management-lifecycle-program.

2009. MAY 8, 2013, What is Vulnerability Management Anyway? , from http://www.tripwire.com/state-of-security/vulnerability-management/what-is-vulnerability-management-anyway/.

2010. Vulnerability Management Life Cycle, from http://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm.

2011. Diana Kelley, Framework for building a vulnerability management lifecycle, program http://searchsecurity.techtarget.com/magazineContent/Framework-for-building-a-vulnerability-management-lifecycle-program.

2012. Asset Prioritization, from http://www.maxhon.com/AP.htm.

2013. Vulnerability Management Prioritize, from https://www.qualys.com/enterprises/qualysguard/vulnerability-management/features/#prioritize.

2014. Tony Martin-Vegue , What's the difference between a vulnerability scan, penetration test and a risk analysis?, from http://www.csoonline.com/article/2921148/network-security/whats-the-difference-between-a-vulnerability-scan-penetration-test-and-a-risk-analysis.html.

2015. Network Vulnerability Assessment, from https://www.riskbasedsecurity.com/penetration-tests/.

2016. Vulnerability Assesment, from http://cdn.ttgtmedia.com/searchEnterpriseLinux/downloads/285_NSS_01.pdf.

2017. Brandan Blevins, What should enterprises look for in vulnerability assessment tools?, from http://searchsecurity.techtarget.com/feature/What-should-enterprises-look-for-in-vulnerability-assessment-tools.

2018. VULNERABILITY ASSESSMENT SERVICES, from http://www.escope.net/escope/vulnerability.aspx.

2019. Kellep Charles (Oct 18, 2012), The Security Vulnerability Assessment Process & Best Practices, http://www.slideshare.net/kellepc/the-security-vulnerability-assessment-process-best-practices.

2020. External Vulnerability Scanning Services, from https://controlcase.com/managed_compliance_pci_vulnerability_scan.html.

2021. Vulnerabilities, Threats, and Attacks, from http://www.lovemytool.com/files/vulnerabilities-threats-and-attacks-chapter-one-7.pdf.

2022. qualys Vulnerability Management, features from https://www.qualys.com/enterprises/qualysguard/vulnerability-management/features/.

2023. April 5 2015, from http://static.tenable.com/documentation/nessus_6.4_user_guide.pdf.

2024. Nessus (software) , from https://en.wikipedia.org/wiki/Nessus_(software).

2025. July 8, 2016, Qualys Cloud Platform Evaluator's Guide, from https://www.qualys.com/docs/qualys-evaluators-guide.pdf.

2026. Operationalize Vulnerability and Risk Management — On Demand, from https://www.securusglobal.com/lib/file/QG_VM_for_ENT_DS.pdf.

2027. Identifying and Mitigating Multiple Vulnerabilities in Network Time Protocol, from https://tools.cisco.com/security/center/viewAMBAlert.x?alertId=36857.

2028. Guide to Effective Remediation of Network Vulnerabilities, from https://www.qualys.com/docs/guide_vulnerability_management.pdf.

2029. Continuous Vulnerability Assessment & Remediation Guideline, from https://security.berkeley.edu/continuous-vulnerability-assessment-remediation-guideline.

2030. Julia Dutton, The Risk Treatment Plan, from https://www.vigilantsoftware.co.uk/blog/author/jdutton.

2031. Dejan Kosutic, Risk Treatment Plan and risk treatment process – What's the difference?, from https://advisera.com/27001academy/knowledgebase/risk-treatment-plan-and-risk-treatment-process-whats-the-difference/.

2032. Risk Treatment Options, Planning and Prevention, from https://resources.infosecinstitute.com/risk-treatment-options-planning-prevention/#gref.

2033. Risk Based Testing: Approach, Matrix, Process & Examples, from https://www.guru99.com/risk-based-testing.html.

2034. Risk Identification, from https://web.actuaries.ie/sites/default/files/erm-resources/risk_identification.pdf.

2035. Gary Stoneburner, Alice Goguen, and Alexis Feringa, from Risk Management Guide for Information Technology Systems, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf.

2036. Key risk indicator, from https://en.wikipedia.org/wiki/Key_risk_indicator.

2037. The Power of Key Risk Indicators (KRIs) in Enterprise Risk Management (ERM), from https://www.metricstream.com/insights/Key-Risk-indicators-ERM.htm.

2038. Kseniya Strachnyi, Operational risk: key risk indicators (KRIs), from https://www.workiva.com/blog/operational-risk-key-risk-indicators-kris.

2039. Guide for Conducting Risk Assessments, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

2040. Vulnerability management, from https://en.wikipedia.org/wiki/Vulnerability_management.

2041. Threat and Vulnerability Management, from https://nigesecurityguy.wordpress.com/2013/06/20/threat-and-vulnerability-management/.
2042. Arnab Roy Chowdhury, Network asset discovery and why you need it for your applications, from https://blog.sqreen.com/network-asset-discovery-and-why-you-need-it-for-your-applications/.
2043. 10 Components of An Effective Vulnerability Management Process, from http://www.itbriefcase.net/10-components-of-an-effective-vulnerability-management-process.
2044. Assets and Groups, from https://cybersecurity.att.com/documentation/usm-appliance/asset-management/about-assets-and-groups.htm.
2045. Katharina Gerberding, The Difference Between Vulnerability Assessments and Vulnerability Management, https://www.hitachi-systems-security.com/blog/difference-vulnerability-assessments-vulnerability-management/.
2046. Need an external network vulnerability assessment?, from https://frsecure.com/external-network-vulnerability-assessment/#toggle-id-2.
2047. Jarred White, Internal vs. External Vulnerability Scans: Why You Need Both, from https://www.pcicomplianceguide.org/internal-vs-external-vulnerability-scans-and-why-you-need-both/.
2048. Attack Trees, from https://www.oreilly.com/library/view/threat-modeling-designing/9781118810057/9781118810057c04.xhtml.
2049. Threat Modeling Using Attack Trees, from https://www.researchgate.net/publication/234738557_Threat_Modeling_Using_Attack_Trees.
2050. Attack Tree Modeling in AttackTree, from https://www.isograph.com/software/attacktree/creating-an-attack-tree/#:~:text=Attack%20tree%20analysis%20provides%20a,those%20attacks%20achieving%20their%20goal.
2051. Nataliya Shevchenko (03 Dec 2018), Threat Modeling: 12 Available Methods, from https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.
2052. Identify the need for a DPIA, from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/dpia-tools/online-retail/step-1-identify-the-need-for-a-dpia/.
2053. How Do Privacy Impact Assessments Work, from https://safetyculture.com/topics/privacy-impact-assessment/.
2054. Paul Kirvan, Privacy Impact Assessment, from https://www.techtarget.com/searchsecurity/definition/privacy-impact-assessment-PIA.
2055. Privacy Impact Assessment, from https://en.wikipedia.org/wiki/Privacy_Impact_Assessment.
2056. Why You Need a PIA, from https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/privacy/privacy-impact-assessments#:~:text=Why%20You%20Need%20a%20PIA,or%20use%20in%20your%20project.
2057. David Harrington (16 Jun 2023), What Is a Privacy Impact Assessment (PIA), from https://www.varonis.com/blog/privacy-impact-assessment#:~:text=PIA%20is%20a%20leading%20risk,safeguard%20private%20or%20confidential%20information.
2058. Automate your privacy and security compliance assessments, from https://www.mandatly.com/products/privacy-assessments.
2059. Pioneering Privacy Impact Assessment Solutions for a Data-Driven World, from https://grcviewpoint.com/seers/.
2060. Privacy Risk Assessments: DPIAs and PIAs, from https://www.clarip.com/data-privacy/privacy-risk-assessment/.
2061. Risk assessments: what they are, why they're important and how to complete them, from https://www.britsafe.org/training-and-learning/find-the-right-course-for-you/informational-resources/risk-assessment/#:~:text=A%20suitable%20and%20sufficient%20risk,the%20task%2Factivity%20in%20question.
2062. Will Kenton (12 Jul 2022), Risk Assessment Definition, Methods, Qualitative Vs. Quantitative, from https://www.investopedia.com/terms/r/risk-assessment.asp.
2063. Privacy Impact Assessment, from https://cyberdatapros.com/privacy-impact-assessment/.
2064. How do you conduct a privacy impact assessment for your web project, from https://www.linkedin.com/advice/0/how-do-you-conduct-privacy-impact-assessment.

Module 19 Threat Assessment with Attack Surface Analysis

2065. LILY HAY NEWMAN, from What Is an Attack Surface?, https://www.wired.com/2017/03/hacker-lexicon-attack-surface/.
2066. Margaret Rouse, attack surface, from https://whatis.techtarget.com/definition/attack-surface.
2067. Attack Surface: Concept, Types, Tools and Reduction Strategies, from https://securitytrails.com/blog/attack-surface.
2068. Attack Surface, from https://www.techopedia.com/definition/33810/attack-surface.
2069. Attack Surface And Attack Vectors, from http://timenetindia.com/blog-2/.
2070. Minimize Software Attack Surfaces for Stronger Security, from https://www.computereconomics.com/article.cfm?id=1337.
2071. Jason Taylor, Reducing Your Application's Attack Surface, from https://blog.securityinnovation.com/blog/2011/02/reducing-your-applications-attack-surface.html.
2072. Reduce cyber threats with Visualizing Attack Surface, from https://www.esoftload.info/reduce-cyber-threats-visualizing-attack-surface.
2073. Josh Mayfield, Reduce Your Attack Surface: Visualize Vulnerabilities, from https://www.firemon.com/reduce-attack-surface-visualize-vulnerabilities/.
2074. Reduce your attack surface: Remove exposures before they become exploits, from https://www.firemon.com/reduce-your-attack-surface/.
2075. What is Attack Surface Analysis and Why is it Important?, from https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html.
2076. Reduce cyber threats with Visualizing Attack Surface, from https://www.esoftload.info/reduce-cyber-threats-visualizing-attack-surface.
2077. Transforming what's possible in cybersecurity management, from https://www.skyboxsecurity.com/.
2078. Shannon Ragan, Indicators of Exposure: Skybox pioneers new approach to reducing the attack surface, from https://blog.skyboxsecurity.com/indicators-of-exposure-skybox-pioneers-new-approach-to-reducing-the-attack-surface/.

2079. What 'Indicators of Exposure' Reveal, from https://www.bankinfosecurity.com/interviews/what-indicators-exposure-reveal-i-3237.
2080. Indicators of Exposure Reference, from https://alsid.com/indicator-exposures-reference.
2081. Indicators of Exposure and Attack Surface Visualization, from https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/sponsored-feature-indicators-of-exposure-and-attack-surface-visualization.
2082. System Attack Surface: Identifying IoEs using Attack Surface Analyzer, from www.microsoft.com.
2083. Identifying IoEs using Windows Sandbox Attack Surface Analysis Tool, from www.owasp.org.
2084. Sandbox Attack Surface Analysis Tools, from https://opensource.google/projects/sandbox-attacksurface-analysis-tools.
2085. James Forshaw, Windows Sandbox Attack Surface Analysis, from https://googleprojectzero.blogspot.com/2015/11/windows-sandbox-attack-surface-analysis.html.
2086. Will Chatham, OWASP Attack Surface Detector Project, from https://www.willchatham.com/tech/owasp-attack-surface-detector-project/.
2087. OWASP Attack Surface Detector, from https://owasp.org/www-project-attack-surface-detector/.
2088. Real-Time Attack Surface Analysis, from https://threatmodeler.com/attack-surface/.
2089. A Secure SDLC Starts With Threat Modeling Software, from https://threatmodeler.com/threat-modeling-software-identifying-sdlc-threats/.
2090. Attack Simulation using Infection Monkey, from www.guardicore.com.
2091. DANIEL MIESSLER, amass — Automated Attack Surface Mapping, from https://danielmiessler.com/study/amass/.
2092. SPF, from https://github.com/tatanus/SPF.
2093. Phishing Campaign, from https://www.barracuda.com/glossary/phishing-campaign.
2094. Disable or enable Java or JavaScript in your browser, from https://kb.iu.edu/d/bcyv#FIREFOXN.
2095. Reducing the Attack Surface of the Web Server, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc785139(v=ws.10)?redirectedfrom=MSDN.
2096. How to disable NetBIOS over TCP/IP by using DHCP server options, from https://support.microsoft.com/en-in/help/313314/how-to-disable-netbios-over-tcp-ip-by-using-dhcp-server-options.
2097. Tom Olzak, Attack Surface Reduction – Chapter 4, from https://resources.infosecinstitute.com/attack-surface-reduction/#gref.
2098. Real-Time Attack Surface Analysis, from https://threatmodeler.com/attack-surface/.
2099. Jason Taylor, Reducing Your Application's Attack Surface, from https://blog.securityinnovation.com/blog/2011/02/reducing-your-applications-attack-surface.html.
2100. Enhanced Mitigation Experience Toolkit (EMET) ASR, from www.microsoft.com.
2101. The Enhanced Mitigation Experience Toolkit, from https://support.microsoft.com/en-in/help/2458544/the-enhanced-mitigation-experience-toolkit.
2102. Margaret Rouse, Microsoft Enhanced Mitigation Experience Toolkit (EMET), from https://searchsecurity.techtarget.com/definition/Microsoft-Enhanced-Mitigation-Experience-Toolkit-EMET.
2103. Enhanced Mitigation Experience Toolkit, from https://en.wikipedia.org/wiki/Enhanced_Mitigation_Experience_Toolkit.

Module 20 Threat Prediction with Cyber Threat Intelligence

2104. What are Indicators of Compromise (IoCs)?, from https://cyware.com/educational-guides/cyber-threat-intelligence/what-are-indicators-of-compromise-iocs-2f0d.
2105. Kallie Marley, Indicators of Compromise (IOCs): Definition and Examples, from https://gadellnet.com/blog/indicators-of-compromise/.
2106. Indicator of compromise, from https://en.wikipedia.org/wiki/Indicator_of_compromise.
2107. What are Indicators of Compromise?, from https://www.forcepoint.com/cyber-edu/indicators-compromise-ioc.
2108. Nate Lord, What are Indicators of Compromise?, from https://digitalguardian.com/blog/what-are-indicators-compromise.
2109. Rohit D Sadgune / Amruta Sadgune, Indicator of Attack vs Indicator of Compromises, from https://hackforlab.com/indicator-of-attack-vs-indicators-of-compromises/.
2110. Indicators of Compromise, from https://www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise.
2111. Understanding Indicators of Attack vs Compromise, from https://capsule8.com/resource/indicators-of-compromise-vs-attack/.
2112. Ken Dunham, IoC and IoA: Indicators of Intelligence, from https://www.optiv.com/blog/ioc-and-ioa-indicators-intelligence.
2113. Jessica DeCianno, IOC Security: Indicators of Attack vs. Indicators of Compromise, from https://www.crowdstrike.com/blog/indicators-attack-vs-indicators-compromise/.
2114. Threat Intelligence: Threat Feeds, Tools, and Challenges, ORION CASSETTO, from https://www.exabeam.com/siem/4-layers-threat-intelligence/.
2115. Drew Robb, Eight Top Threat Intelligence Platforms, from https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html.
2116. Top Hacking Forums, from http://www.effecthacking.com/2015/11/top-hacking-forums.html.
2117. Hack Forums, from https://en.wikipedia.org/wiki/Hack_Forums.
2118. 10 Best Deep Web Hacker Forums, from https://www.deepwebsiteslinks.com/hacker-forums/.
2119. ORION CASSETTO, from Threat Intelligence: Threat Feeds, Tools, and Challenges, https://www.exabeam.com/siem/4-layers-threat-intelligence/.

2120. Importance of Threat Intelligence (TI) And Feeds, from https://www.cm-alliance.com/cybersecurity-blog/importance-of-threat-intelligence-feeds.
2121. Threat Intelligence: What Is It, And How Can It Protect You From Today's Advanced Cyber-Attacks?, from https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf.
2122. ZANE POKORNY, Threat Intelligence Feeds: Overview, Best Practices, and Examples, from https://www.recordedfuture.com/threat-intelligence-feeds/.
2123. How to use Cisco Threat Intelligence Director on the Firepower Management Center, from https://steemit.com/cisco/@cydera/how-to-use-cisco-threat-intelligence-director-on-the-firepower-management-center.
2124. AlienVault Threat Intelligence, from https://cybersecurity.att.com/solutions/threat-intelligence.
2125. Dynamic Threat Intelligence (DTI) service, from www.fireEye.com.
2126. Insights tailored to your business (SurfWatch), from www.hackSurfer.com.
2127. Threat feeds from their big data solution ActiveTrust (Infoblox), from www.internetIdentity.com.
2128. Real-time threat intelligence from the web, from www.recordedFuture.com.
2129. DeepSight feeds on a variety of topics including reputation, from www.symantec.com.
2130. Everything there is to know about the past, present, and future of spies, from www.spytales.com.
2131. Enterprise Detection & Response, from https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.
2132. Veronica Drake (06 Jul 2022), The Pyramid of Pain and Cyber Threat Intelligence, from https://flashpoint.io/blog/the-pyramid-of-pain-and-cyber-threat-intelligence/.
2133. Threat Intelligence and The Pyramid of Pain, from https://www.netsurion.com/articles/the-pyramid-of-pain.
2134. The Concept of Pyramid of Pain, from https://cyware.com/security-guides/cyber-threat-intelligence/the-concept-of-pyramid-of-pain-f358.
2135. FACTORS AFFECTING THE MATURITY LEVEL OF THREAT HUNTING IN SRI LANKA DEFENCE SERVICE: A CASE STUDY IN SRI LANKA NAVY, from https://www.researchgate.net/publication/344319370_FACTORS_AFFECTING_THE_MATURITY_LEVEL_OF_THREAT_HUNTING_IN_SRI_LANKA_DEFENCE_SERVICE_A_CASE_STUDY_IN_SRI_LANKA_NAVY/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6Il9kaXJlY3QiLCJwYWdlIjoiX2RpcmVjdCJ9fQ.
2136. Mohamed Kasim (25 Sep 2020), Threat hunting for Beginners, from https://www.slideshare.net/SKMohamedKasim/sk-threat-hunting.
2137. 28 Oct 2015, The Threat Hunting Reference Model, from https://www.threathunting.net/files/The%20Threat%20Hunting%20Reference%20Model%20Part%202_%20The%20Hunting%20Loop%20_%20Sqrrl.pdf.
2138. Splunk Threat Hunting Workshop, from https://www.slideshare.net/Splunk/slunk-threat-hunting-workshop.
2139. Robert M. Lee (Feb 2016), The Who, What, Where, When, Why and How of Effective Threat Hunting, from https://sansorg.egnyte.com/dl/vlw6oNZbnj.
2140. Splunk Threat Hunting Workshop, from https://www.slideshare.net/Splunk/slunk-threat-hunting-workshop.
2141. Oleksandra Rumiantseva (10 Aug 2022), What is Threat Hunting Maturity Model, from https://socprime.com/blog/threat-hunting-maturity-model-explained-with-examples/#What_is_Threat_Hunting_Maturity_Model.
2142. Managed Protection, Detection and Response, from https://mantix4.com/solutions-overview/.
2143. Detect and Respond to Advanced Attacks, from https://www.vmware.com/in/products/endpoint-detection-and-response.html.
2144. Exabeam Fusion, from https://www.exabeam.com/product/fusion/.
2145. Threat Hunting, from https://help.cynet.com/en/articles/54-threat-hunting.
2146. What are some of the innovative ways that incident handlers use artificial intelligence and machine learning, from https://www.linkedin.com/advice/0/what-some-innovative-ways-incident-handlers-use.
2147. AI in Cybersecurity: Incident Response Automation Opportunities, from https://www.sisainfosec.com/blogs/ai-in-cybersecurity-incident-response-automation-opportunities/.
2148. Theresa Foley (02 Mar 2023), Ushering in AI to Automate Cyber Threat Intelligence, from https://www.mimecast.com/blog/ushering-in-ai-to-automate-cyberthreat-intelligence/.
2149. Sonya Moisset, How Security Analysts Can Use AI in Cybersecurity, from https://www.freecodecamp.org/news/how-to-use-artificial-intelligence-in-cybersecurity/.
2150. Beenu Arora, How AI-Enabled Threat Intelligence Is Becoming Our Future, from https://www.forbes.com/sites/forbestechcouncil/2023/07/21/how-ai-enabled-threat-intelligence-is-becoming-our-future/?sh=33160e05727ehttps://h2o.ai/wiki/ai-models/#:~:text=An%20artificial%20intelligence%20(AI)%20model,it%20receives%20multiple%20data%20points.
2151. Cyber Threat Intelligence, from https://www.neteye-blog.com/2021/10/cyber-threat-intelligence-enrichment-with-satayo-ioc/.
2152. Automated Threat Intelligence Enrichment, from https://cyware.com/use-case/automated-threat-intelligence-enrichment.
2153. Anusthika Jeyashankar (21 March 2022), IOC vs IOA: Indicators of Threat Intelligence, from https://www.socinvestigation.com/ioc-vs-ioa-indicators-of-threat-intelligence/.
2154. 10 May 2023, What are Indicators of Compromise in Threat Intelligence, from https://flare.io/learn/resources/blog/indicators-of-compromise-threat-intelligence/.
2155. Using Threat Intelligence to Defend Against Phishing and Fraud Campaigns, from https://www.bitdefender.com/blog/businessinsights/using-threat-intelligence-to-defend-against-phishing-and-fraud-campaigns/.
2156. Artificial intelligence (AI) cybersecurity, from https://www.ibm.com/id-en/security/artificial-intelligence.

2157. Threat Intelligence Management, Elevated, from https://www.paloaltonetworks.com/cortex/threat-intel-management.
2158. Threat Intelligence Operations Platform, from https://threatconnect.com/threat-intelligence-platform/.
2159. Threat Intelligence Tools, from https://www.bluevoyant.com/knowledge-center/threat-intelligence-tools-types-benefits-and-best-practices.
2160. Guidelines for the secure and ethical use of Artificial Intelligence, from https://itsecurity.uiowa.edu/guidelines-secure-and-ethical-use-artificial-intelligence.
2161. Michael McKenna, Machines and Trust: How to Mitigate AI Bias, from https://www.toptal.com/artificial-intelligence/mitigating-ai-bias.

APPENDIX A Computer Network Fundamentals

2162. Ms. Mousami Pawar (Dec 5, 2014), Network Security, from http://www.slideshare.net/mousmip/network-security fundamental.
2163. Internet and Internet Communication(s) (June 2012), from https:// ccdcoe.org/ cycon/ 2012/ workshops/ Internet_ Internet_ Comms.pdf.
2164. John E. Canavan, Fundamentals of Network Security, from http://www.askcypert.org/sites/default/files/Canavan_J.E._Fundamentals_of_network_security_(2001)(en)(218s).pdf.
2165. DoDD 8570.1: Blue Team, from https://www.sypriselectronics.com/information-security/cyber-security solutions/computer-network-defense/.
2166. Mariusz Stawowski (ISSA Journal October 2007), The Principles of Network Security Design, from http:// www.clico.pl/services/ Principles_Network_Security_Design.pdf.
2167. Diane Teare, Designing for Cisco Internetwork Solutions (DESGN), from http:// portal.aauj.edu/ portal_resources/ downloads/ networking/ designing_network_security_cisco_press.pdf.
2168. Types of Network, from http://www.codesandtutorials.com/networking/basics/computer_network-types.php.
2169. Department of Defense (March 9 , 2001, Support to Computer Network Defense (CND), from https://info.publicintelligence.net/DoD-SupportCND.pdf.
2170. Computer Network Defense, from https://www.safaribooksonline.com/library/view/cyberwarfare 2nd/9780124166721/xhtml/CHP011.html.
2171. Computer Network Defense (CND), from https://www.techopedia.com/definition/27906/computer-network-defense-cnd.
2172. Computer security, from https://en.wikipedia.org/wiki/Computer_security.
2173. What is Information Security? From http://demop.com/articles/what-is-information-security.pdf.
2174. Computer network operations, from https://en.wikipedia.org/wiki/Computer_network_operations.
2175. Margaret Rouse,(Feb 2015), authentication, from http://searchsecurity.techtarget.com/definition/authentication.
2176. 5 Core Principles of Information Assurance (May 23, 2011), from https://onlinebusinesscertificates.wordpress.com/2011/05/23/5-core-principles-of-information-assurance/.
2177. NSA(CSS), Information Assurance, from https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
2178. Trusted Information Sharing Network for critical infrastructure protection (June 208), from http://www.qcert.org/sites/default/files/public/documents/au-bp-defence_in_depth-eng-2008.pdf.
2179. physical security , from http://searchsecurity.techtarget.com/definition/physical-security.
2180. Vanessa Frias-Martinez, Joseph Sherrick,Salvatore J. Stolfo, Angelos D. Keromytis, A Network Access Control Mechanism Based on Behavior Profiles, from https:// www.cs.columbia.edu/ ~angelos/ Papers/ 2009/acsac09.pdf.
2181. Ajay Yadav (April 1 2013), Network Design: Firewall, IDS/IPS, from http://resources.infosecinstitute.com/network-design firewall-idsips/.
2182. Tony Bradley, Proxy Server, from http://netsecurity.about.com/cs/generalsecurity/g/def_proxy.htm.
2183. Hardening (computing), from https://en.wikipedia.org/wiki/Hardening_(computing).
2184. Packet Filtering, from https://www.techopedia.com/definition/4038/packet-filtering.
2185. Margaret Rouse(March 2001), Common Criteria (CC) for Information Technology Security Evaluation, from
2186. http://whatis.techtarget.com/definition/Common-Criteria-CC-for-Information-Technology-Security-Evaluation.
2187. GERALD J. POPEK AND CHARLES S. KLINE, Encryption and Secure Computer Networks , from http://www.cs.swarthmore.edu/ ~newhall/readings/popek.pdf.
2188. Feb 2008, Password management , from http://www.infosec.gov.hk/english/technical/files/password.pdf.
2189. Deb Shinder (August 28, 2001), Understanding and selecting authentication methods, from http://www.techrepublic.com/article/ understanding-and-selecting-authentication-methods/.
2190. network configuration management (NCM) , from http://searchnetworking.techtarget.com/definition/network configuration-management.
2191. Network Security Audit – Multi platform consolidation with security event corelation, from http://www.enforcive.com/network-security-audit.
2192. Frederick M. Avolio (July 2007), Producing your network security policy, from https:// www.watchguard.com /docs/whitepaper /securitypolicy_wp.pdf.
2193. STANDARD OPERATING PROCEDURES, http://www.fao.org/docrep/w7295e/w7295e04.htm.
2194. Padmavathy Ramesh (July 2002), Business Continuity Planning, from http://www.tcs.com/SiteCollectionDocuments/ White%20Papers/Business%20Continuity%20Planning.pdf.
2195. Configuration Control, from http://www.chambers.com.au/glossary/configuration_control.php.

2196. Relevant Incident Response, from https://books.google.co.in/books?id=6lJxGXfLWkYC&pg=PA234&lpg=PA234&dq=Conducting+forensics+activities++on+incidents&source=bl&ots=pjOtZSKdDK&sig=1LH6RbO1tIhH5OS8ehOs9xHKUU4&hl=en&sa=X&ved=0CDUQ6AEwBGoVChMIxofau8OcyQIV0m2OCh2O5Akh#v=onepage&q=Conducting%20forensics%20activities%20%20on%20incidents&f=false.

2197. August 2000, Security Culture: a handbook for activists, from http://www.animalliberationfront.com/ALFront/ELF/sec handbook.pdf.

2198. Jennifer Pfeffer (7/11/2016), What Does a Network Administrator Do? A Behind-the-Scenes Look, from http://www.rasmussen.edu/ degrees/ technology/ blog/what-does-a-network-administrator-do/.

2199. Protecting Data in a Network Environment, from https://docs.oracle.com/cd/B12037_01/network.101/b10777/protnet.htm.

2200. Architecture Overview, http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm#wp42293.

2201. Nimmy Reichenberg (September 26, 2013), Four Tips for Designing a Secure Network Perimeter, from http://www.securityweek.com/four-tips-designing-secure-network-perimeter.

2202. Incident Response Plan, from http://www.comptechdoc.org/independent/security/policies/incident-response-plan.html.

2203. 6 November, 2015, Responding to Network Attacks and Security Incidents, from http://www.tech-faq.com/responding-to network-attacks-and-security-incidents.html.

2204. The Difference Between Events, Alerts, and Incidents, from https://danielmiessler.com/study/event-alert-incident/.

2205. Vulnerabilities, Threats, and Attacks, from http://www.lovemytool.com/files/vulnerabilities-threats-and-attacks-chapter one-7.pdf.

2206. Responding to Network Attacks and Security Incidents, from http://www.tech-faq.com/responding-to-network-attacks and-security-incidents.html.

2207. Red Team/Blue Team, Capture the Flag, and Treasure Hunt: Teaching Network Security Through Live Exercises , from http://ictf.cs.ucsb.edu/pdfs/2003_WISE_iCTF.pdf.

2208. Cyril Onwubiko (13th December 2011), Computer Network Defense Approaches, from http://www.research-series.com/

2209. cyril/ Approaches%20in%20security%20defense.pdf.

2210. personal area network (PAN), from http://searchmobilecomputing.techtarget.com/definition/personal-area-network.

2211. Personal area network, from https://en.wikipedia.org/wiki/Personal_area_network.

2212. The CentOS Project, from https://www.centos.org .

2213. TCP/IP Overview and History , from http://www.tcpipguide.com/free/t_TCPIPOverviewandHistory.htm.

2214. THE TCP/IP PROTOCOL SUITE, from http://www.exa.unicen.edu.ar/catedras/comdat1/material/TP1-Ejercicio5-ingles.pdf.

2215. What is TCP/IP?, from http://www.uic.edu/depts/accc/network/ftp/v452.html#whatis.

2216. The Internet Transport Protocols: TCP, from http:// eee.guc.edu.eg/ Courses/ Networks/NETW901%20Local%20Area%20Networks/Lectures/TCP.pdf.

2217. half-duplex and full-duplex Ethernet vs Switches and Hubs, from http://queryd.com/questions/full-duplex.html.

2218. Media session framework using a control module to direct and manage application and service servers, from http://www.google.co.in/patents/US7185094.

2219. Transmission Control Protocol , from https://en.wikipedia.org/wiki/Transmission_Control_Protocol.

2220. TCP Operation, from http://www.freesoft.org/CIE/Course/Section4/7.htm.

2221. TCP Basic Operation: Connection Establishment, Management and Termination , from http:// www.tcpipguide.com/ free/t_TCPBasicOperationConnectionEstablishmentManagement.htm.

2222. Explain TCP and UDP operations, from http://www.examcollection.com/certification-training/ccnp-explain-tcp-and-udp operations.html.

2223. Basic TCP operation, from https://niktips.wordpress.com/2012/06/06/basic-tcp-operation/.

2224. Transmission Control Protocol, from https://en.wikipedia.org/wiki/Transmission_Control_Protocol .

2225. TCP Connection Establishment Process: The "Three-Way Handshake" , from http:// www.tcpipguide.com/ free/t_TCPConnectionEstablishmentProcessTheThreeWayHandsh.htm.

2226. Kartik Krishnan (2004), User Datagram Protocol (UDP):, from http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture5.pdf.

2227. UDP - User Datagram Protocol, from http://ipv6.com/articles/general/User-Datagram-Protocol.htm.

2228. UDP Overview, History and Standards, from http://www.tcpipguide.com/free/t_UDPOverviewHistoryandStandards.htm.

2229. The Transmission Control Protocol (TCP), from https://books.google.co.in/books?id=Ts4SKa6qLLYC&pg=PA169&lpg=PA169&dq=TCP+operation&source=bl&ots=zsLXikzEMs&sig=UkSA7bvWnG tyyMJ8Tp4AjiPG5g&hl=en&sa=X&ved=0CBsQ6AEwADgKahUKEwidjsz035vJAhUVkI4KHWjDBW8#v=onepage&q=TCP%20operation&f=false.

2230. UDP Operation, from http://www.tcpipguide.com/free/t_UDPOperation.htm.

2231. Explain UDP operations, from http://ccieordie.com/1-1-f-explain-udp-operations/.

2232. Nick (August 20, 2014),CCIE Written Blueprint: 1.1.f Explain UDP operations, from https:// www.geekynick.co.uk/1-1-f explain-udp-operations/.

2233. UDP Operations, from http://www.hackandtinker.net/2014/12/17/udp-operations/.

2234. IP header, from https://en.wikipedia.org/wiki/IP_header.

2235. IP Internet Protocol, from http://www.networksorcery.com/enp/protocol/ip.htm.

2236. Himanshu Arora (26 March 2012), Protocol Header Fundamentals Explained with Diagrams, from http://www.thegeekstuff.com/2012/03/ip-protocol-header/.
2237. Internet Addressing and Routing First Step, from http:// www.ciscopress.com/ articles/ article.asp?p=348253&seqNum=4.
2238. Internet Protocol IP Datagram, Fragmentation and Reassembly, from http://user.it.uu.se/~rmg/teaching/IP.pdf.
2239. IP Packet Structure, from http://www.freesoft.org/CIE/Course/Section3/7.htm.
2240. INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION (September 1981), from https://tools.ietf.org/html/rfc791.
2241. Tech Info - IP Message Formats, from http://www.zytrax.com/tech/protocols/tcp.html.
2242. IP Datagram General Format, from http://www.tcpipguide.com/free/t_IPDatagramGeneralFormat.htm.
2243. IP Datagram Options and Option Format , from http://www.tcpipguide.com/free/t_IPDatagramOptionsandOptionFormat.htm.
2244. IPv4 Packet Header, from http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/ip-packet.html.
2245. IP (Internet Protocol), from https://www.lri.fr/~fmartignon/documenti/reseauxavances/2-IP-Martignon.pdf.
2246. Vangie Beal, IPng - IPv6 (Internet Protocol Version 6), from http://www.webopedia.com/TERM/I/IPng.html.
2247. IPv6, from https://en.wikipedia.org/wiki/IPv6.
2248. IPv6, from http://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6.
2249. What is IPv6?, from https://support.apple.com/en-us/HT202236.
2250. Kaushik Das, IPv6 - The Next Generation Internet, from http:// www.ipv6.com/articles/general/ipv6-the-next-generation internet.htm.
2251. Kaushik Das, A Beginner's Look into IPv6, from http://ipv6.com/articles/general/IPv6-Beginners_Look.htm.
2252. IPv6 Tutorial, from http://www.tutorialspoint.com/ipv6/.
2253. Frequently asked questions on IPV6, from https://www.google.com/intl/en/ipv6/faq.html.
2254. TCP/IP v4 and v6, from https://technet.microsoft.com/en-us/network/bb530961.aspx.
2255. IPv6 packet, from https://en.wikipedia.org/wiki/IPv6_packet.
2256. IPv6 – Headers, from http://www.tutorialspoint.com/ipv6/ipv6_headers.htm.
2257. Kaushik Das , IPv6 Header Deconstructed, from http://ipv6.com/articles/general/IPv6-Header.htm.
2258. IPv6 Datagram Main Header Format , from http://www.tcpipguide.com/free/t_IPv6DatagramMainHeaderFormat.htm.
2259. October 2006, IPv6 Extension Headers Review and Considerations, from http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html.
2260. Internet Protocol, Version 6 (IPv6) Specification, from https://tools.ietf.org/html/rfc2460.
2261. IPv6 Internet Protocol Version 6, from http://www.networksorcery.com/enp/protocol/ipv6.htm.
2262. IPv6 Datagram Header Format, from http://www.omnisecu.com/tcpip/ipv6/ipv6-datagram-header-format.php.
2263. IP V6 Header, from http://euclid.nmu.edu/~rappleto/Classes/CS442/Notes/IPv6_Header.html.
2264. IPv6 transition mechanism, from https://en.wikipedia.org/wiki/IPv6_transition_mechanism.
2265. April 21, 2009, IPv6 Transition Mechanisms and Strategies http://www.rmv6tf.org/wp-content/uploads/2012/11/Chuck Sellers-090421-IPv6-Transition-Mechanisms-Sellers1.pdf.
2266. Making the Transition From IPv4 to IPv6 (Reference) , from https://docs.oracle.com/cd/E19683-01/817-0573/transition 10/index.html.
2267. Basic Transition Mechanisms for IPv6 Hosts and Routers, from https://tools.ietf.org/html/rfc4213.
2268. Transition Mechanisms, from http://portalipv6.lacnic.net/en/transition-mechanisms/.
2269. Kaushik Das , IPv6 Transition Technologies, from http://ipv6.com/articles/gateways/IPv6-Tunnelling.htm.
2270. Todd Lammle, CISCO Certified Network Associate Study Guide, 5th Edition, from http:// www.cs.rpi.edu/ ~kotfid/ne1/ CCNA_chapter2.pdf .
2271. Dynamic Host Configuration Protocol, from https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol.
2272. Vangie Beal, DHCP - Dynamic Host Configuration Protocol, from http://www.webopedia.com/TERM/D/DHCP.html .
2273. What is DHCP?, from https://kb.iu.edu/d/adov.
2274. DHCP (Dynamic Host Configuration Protocol) , from http://searchunifiedcommunications.techtarget.com/definition/DHCP.
2275. What is DHCP?, from http://whatismyipaddress.com/dhcp.
2276. Dynamic Host Configuration Protocol (DHCP), from https://www.freebsd.org/doc/handbook/network-dhcp.html.
2277. Configure DHCP options , from ftp://ftp1.digi.com/support/documentation/appnote_dhcpoptions.pdf.
2278. Dynamic Host Configuration Protocol for IPv6 (DHCPv6), from https://www.rfc-editor.org/rfc/rfc3315.txt.
2279. DHCP Message Format, from http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm.
2280. Dynamic Host Configuration Protocol, from http://www.tarunz.org/~vassilii/TAU/protocols/dhcp/frame.htm.
2281. Dynamic Host Configuration Protocol (DHCP) Message Format), from http://www.omnisecu.com/tcpip/dhcp-dynamic-host configuration-protocol-message-format.php.
2282. DHCP Header (RFC 2131), from https://www.securitywizardry.com/packets/pdf/dhcp_header.pdf.
2283. MARSHALL BRAIN & STEPHANIE CRAWFORD , How Domain Name Servers Work, from http://computer.howstuffworks.com/dns.htm.
2284. How the Domain Name System (DNS) works, from https://www.bytemark.co.uk/support/document_library/dnsworks/.
2285. March 28 2003, How DNS Workshttps://technet.microsoft.com/en-in/library/cc772774(v=ws.10).aspx.

2286. Srikanth Ramesh, How Domain Name System (DNS) Workshttp://www.gohacking.com/how-dns-works/.
2287. How Anonymous plans to use DNS as a weapon, from http://arstechnica.com/business/2012/03/how-anonymous-plans-to use-dns-as-a-weapon/.
2288. What is DNS?, from https://in.godaddy.com/help/what-is-dns-665.
2289. Domain Name System, from https://en.wikipedia.org/wiki/Domain_Name_System.
2290. Vangie Beal, DNS - Domain Name System, from http://www.webopedia.com/TERM/D/DNS.html.
2291. DNS message format, from http://www.comptechdoc.org/independent/networking/terms/dns-message-format.html.
2292. DNS Packet Structure , from http://www.ccs.neu.edu/home/amislove/teaching/cs4700/fall09/handouts/project1-primer.pdf.
2293. DNS header, from http://www.networksorcery.com/enp/protocol/dns.htm.
2294. DNS Message Header and Question Section Format, from http://www.tcpipguide.com /free/ t_DNSMessageHeaderandQuestionSectionFormat.htm.
2295. DNS QUERY MESSAGE FORMAT, from http://www.firewall.cx/networking-topics/protocols/domain-name-system-dns/160-protocols-dns-query.html.
2296. DNS Messages, from http://www.zytrax.com/books/dns/ch15/.
2297. DNS Protocol , from https://technet.microsoft.com/en-us/library/dd197470(v=ws.10).aspx.
2298. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, from https://www.ietf.org/rfc/rfc1035.txt.
2299. Domain Name System (DNS), from http://www.rhyshaden.com/dns.htm.
2300. Internet Control Message Protocol (ICMP), from http://www.erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/icmp.html.
2301. ICMP, Internet Control Message Protocol, from http://www.networksorcery.com/enp/protocol/icmp.htm.
2302. Swayam Prakasha, Internet Control Message Protocol (ICMP) Explained, from http://www.linuxuser.co.uk/features/internet-control-message-protocol-icmp-explained.
2303. INTERNET CONTROL MESSAGE PROTOCOL, from https://tools.ietf.org/html/rfc792.
2304. Internet Control Message Protocol (ICMP), from https://www.techopedia.com/definition/5362/internet-control-message protocol-icmp.
2305. ICMP (Internet Control Message Protocol), from http://searchnetworking.techtarget.com/definition/ICMP.
2306. Internet Control Message Protocol, from https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol.
2307. ICMP Common Message Format and Data Encapsulation, from http:// www.tcpipguide.com/ free/t_ICMPCommonMessageFormatandDataEncapsulation.htm.
2308. ARP Caching, http://www.tcpipguide.com/free/t_ARPCaching.htm.
2309. Address Resolution Protocol (arp), from http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
2310. Jhemphill (February 18, 2008), ARP cache: What is it and how can it help you?, from https://www.petri.com/csc_arp_cache.
2311. Address Resolution Protocol (ARP), from http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol ARP.
2312. ARP - Address Resolution Protocol, from http://ipv6.com/articles/general/Address-Resolution-Protocol.htm.
2313. Address Resolution Protocol, from https://en.wikipedia.org/wiki/Address_Resolution_Protocol.
2314. ARP Message Format, from http://www.tcpipguide.com/free/t_ARPMessageFormat.htm.
2315. DRAFT: IPv6 Address Allocation and Assignment Policy , from https://www.ripe.net/publications/docs/draft-ipv6-address allocation-and-assignment-policy.
2316. IPv6 Address Allocation and Assignment Policy, from https://www.apnic.net/docs/drafts/ipv6-address-policy-v006.
2317. IPv6 Address Allocation and Assignment Policy, from https://www.arin.net/policy/archive/ipv6_policy.html.
2318. APNIC Internet Number Resource Policies, from https://www.apnic.net/policy/resources.
2319. Internet Resource Management at ICANN and Regional Internet Registries from https://www.ntt review.jp/archive/ntttechnical.php?contents=ntr201003gls.html.
2320. Nathali Trenaman (24 April 2012), ipv6 addressing plan fundamentals, from http://www.slideshare.net/ripencc/ipv6-addressing-plan-fundamentals.
2321. Draft: PA/PI Unification IPv6 Address Space - New Policy Text, from https://www.ripe.net/publications/docs/ripe documents/other-documents/draft-pa-pi-unification-ipv6-address-space-new-policy-text.
2322. IPv6 Address Assignment Example, from https://networklessons.com/ipv6/ipv6-address-assignment-example/.
2323. Subnetwork, from https://en.wikipedia.org/wiki/Subnetwork.
2324. Vangie Beal, subnet mask – subnetting, from http://www.webopedia.com/TERM/S/subnet_mask.html.
2325. subnet mask, from http://searchnetworking.techtarget.com/definition/subnet-mask.
2326. What is a Subnet Mask?, from https://www.iplocation.net/subnet-mask.
2327. Subnet mask, from http://www.computerhope.com/jargon/s/subnetma.htm.
2328. Internet Protocol Tutorial – Subnets, from http://compnetworking.about.com/od/workingwithipaddresses/a/subnetmask.htm.
2329. Subnets and Subnet Masks, from https://technet.microsoft.com/en-us/library/cc958832.aspx.
2330. Subnet Mask, from https://www.techopedia.com/definition/5563/subnet-mask.

2331. IP Address Alocation, from https:// books.google.co.in/ books?id=TzGxd32TKsoC&pg=PA180&lpg=PA180&dq=IP+Address+Allocation+Structure&source=bl&ots=zYlDfS1m89&sig=3Z3NhLB6KBkF15dhEfe4QSt9QZA&hl=en&sa=X&ved=0ahUKEwjckaDhg5_JAhVEGY4KHSoqD_kQ6AEIQjAG#v=onepage&q=IP%20Address%20Allocation%20Structure&f=false.

2332. IPv6 address, from https://en.wikipedia.org/wiki/IPv6_address.

2333. IP Version 6 Addressing Architecture, from https://tools.ietf.org/html/rfc4291.

2334. 28th March 2003, IPv6 Address Types, from https://technet.microsoft.com/en-us/library/cc757359(v=ws.10).aspx.

2335. IPv6 Addressing Architecture, from https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ipv6-addressing-architecture.

2336. IPv6 Addressing Overview, from http://docs.oracle.com/cd/E23823_01/html/816-4554/ipv6-overview-10.html.

2337. Kaushik Das, IPv6 Addressing, from http://ipv6.com/articles/general/IPv6-Addressing.htm.

2338. IPv6 - Address Types & Formats, from http://www.tutorialspoint.com/ipv6/ipv6_address_types.htm.

2339. IPv6 address format, from http://computernetworkingnotes.com/ipv6-features-concepts-and-configurations/ipv6-address types-and-formats.html.

2340. Carla Schroder (Sep 20, 2006), Understand IPv6 Addresses , from http:// www.enterprisenetworkingplanet.com/ netsp/ article.php/3633211/Understand-IPv6-Addresses.htm.

2341. IPv6 Addressing, from https:// www.cisco.com/ en/ US/ technologies/ tk648/ tk872/technologies_white_paper0900aecd8026003d.pdf.

2342. Preparing an IPV6 Address Plan Manual, from http://www.ipv6forum.com/dl/presentations/IPv6-addressing-plan howto.pdf.

2343. Automatic Tunneling https:// books.google.co.in/ books?id=4LMIZi2ODFkC&pg=PA256&lpg=PA256&dq=IPv4+Compatible+IPv6+Address&source=bl&ots=3qlOwSgO6a&sig=7Mi6nhQLos2mlDuKWDiC4AA8axQ&hl=en&sa=X&ved=0ahUKEwiq4ofM9p7JAhUNGo4KHbOGDPI4ChDoAQhHMAk#v=onepage&q=IPv4%20Compatible%20IPv6%20Address&f=false.

2344. IPV4/ IPV6 Addresses , from https:// books.google.co.in/ books?id=Ts4SKa6qLLYC&pg=PA159&lpg=PA159&dq=IPv4+Compatible+IPv6+Address&source=bl&ots=zsLY9kIGIA&sig=cdKcIaunEnEjb6FipbMW7xOdsXM&hl=en&sa=X&ved=0ahUKEwiq4ofM9p7JAhUNGo4KHbOGDPI4ChDoAQhEMAg#v=onepage&q=IPv4%20Compatible%20IPv6%20Address&f=false.

2345. IPv6 Tunneling part 2: IPv4-Compatible IPv6 Tunnels, from http://resources.intenseschool.com/ipv6-tunneling-ipv4-compatible-ipv6-tunnels/.

2346. IPV4 Mapped – IPV6 Addresses https:// books.google.co.in/ books?id=FbYjJjZNA5gC&pg=PA123&lpg=PA123&dq=IPv4+Compatible+IPv6+Address&source=bl&ots=5lGkDJx_TJ&sig=qyIzYAjtSwFTrzGJ39lo7bpm5wI&hl=en&sa=X&ved=0ahUKEwiq4ofM9p7JAhUNGo4KHbOGDPI4ChDoAQg7MAY#v=onepage&q=IPv4%20Compatible%20IPv6%20Address&f=false.

2347. IPv6 Automatic IPv4-Compatible Tunnels, from http://www.cisco.com/c/en/us/td/docs/ios xml/ios/interface/configuration/15-sy/ir-15-sy-book/ip6-auto-comp-tun.pdf.

2348. Using IPv4-Compatible Address Formats , from https://docs.oracle.com/cd/E19683-01/817-0573/transition-4/index.html.

2349. IPv6/IPv4 Address Embedding , from http://www.tcpipguide.com/free/t_IPv6IPv4AddressEmbedding-2.htm.

2350. ISC DHCP Enterprise Grade Solution for Configuration Needs, from https://www.isc.org/downloads/dhcp/.

APPENDIX B Physical Network Security

2351. IT Secuirty, from http://www.polyu.edu.hk/~ags/itsnews0511/security.html.

2352. Tom Eston (Dec 1, 2008), Physical Security Assessments, from http://www.slideshare.net/agent0x0/physical-security assessments-presentation.

2353. Selvadurai Jeyarajah, Computer Security, http://www.doc.ic.ac.uk/~nd/surprise_95/journal/vol2/sj1/article2.html.

2354. PHYSICAL SECURITY TECHNOLOGY , from http://www.perpetuitytraining.com/physicalsecurity.html.

2355. Michael Betancourt, Security Challenges for the New Paradigm, from https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiRoOzfs87KAhWHt44KHX41DyEQFggbMAA&url=http%3A%2F%2Fwww.eecs.ucf.edu%2F~turgut%2FCOURSES%2FEEL6788_AWN_Spr11%2FLectures%2FSecurityChallenges.ppt&usg=AFQjCNEkelSU19Pry3weQl27MtQT1N3V0A&bvm=bv.113034660,d.c2E&cad=rja.

2356. anoir2014 (Apr 8, 2014), Understanding Security Layers, from http://www.slideshare.net/anoir2014/98-367-lesson-1-slides.

2357. Lisa Phifer, Removable storage device endpoint security and control, from http://searchsecurity.techtarget.com/magazineContent/Removable-storage-device-endpoint-security-and-control.

2358. Alan Calder, Steve Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002 , from https://books.google.co.in/books?id=OctwCgAAQBAJ&pg=PA194&lpg=PA194&dq=failure+of+supporting+utilities&source=bl&ots=b6cDcmMH5i&sig=LRTStSiJniQ5_rzy_9SGFiZfdA&hl=en&sa=X&sqi=2&ved=0ahUKEwje_537yOLJAhURA44KHcNCw4Q6AEILjAE#v=onepage&q=failure%20of%20supporting%20utilities&f=false Peter H. Gregory , IT Disaster Recovery

2359. Planning For Dummies, from https://books.google.co.in/books?id=YC49DXW_60C&pg=PA137&lpg=PA137&dq=mantrap+diagram+representation&source=bl&ots=vtplq0ypDb&sig=Ob9lkb1tsu0a2mg0aeVzst0RXw&hl=en&sa=X&sqi=2&ved=0ahUKEwipuJnfzOLJAhVMj44KHWhbA0YQ6AEILTAD#v=onepage&q=mantrap%20diagram%20representation&f=false.

2360. Dhani Ahmad (Mar 17, 2015), Physical security, from http://www.slideshare.net/emolagi/physical-security-45924353.

2361. Tom Rubenoff (March 1, 2014), from http://hubpages.com/technology/How-to-Create-a-Basic-Mantrap-System.

2362. HD X-Ray Inspection Systems, from http://www.us.anritsu-industry.com/x-ray-inspection.aspx.
2363. Material Measurement Laboratory, from http://www.nist.gov/mml/mmsd/security_technologies/diet-conceal.cfm.
2364. Access Control: Models and Methods (NOVEMBER 28, 2012), from http://resources.infosecinstitute.com/access-control models-and-methods/.
2365. Access Control Methodologies (10/12/04), from http://www.jblearning.com/samples/076372677X/chapple02.pdf.
2366. Microsoft TechNet (March 28, 2003), Authorization and Access Control Technologies, https://technet.microsoft.com/en us/library/cc782880(v=ws.10).aspx.
2367. https://technet.microsoft.com/en-us/library/cc782880(v=ws.10).aspx.
2368. Jeff A Sandine (January 20, 2009), What is the Difference Between Tailgating and Piggybacking Through an Access Controlled Secure Door?, from http://ezinearticles.com/?What-is-the-Difference-Between-Tailgating-and-Piggybacking Through-an-Access-Controlled-Secure-Door?&id=1902821.
2369. Mohd Hamizi (May 21, 2015), ensuring physical and data security, http://www.slideshare.net/pdawackomct/3-ensuring physical-and-data-security.
2370. Deb Shinder (July 16, 2007), 10 physical security measures every organization should take, from http://www.techrepublic.com/blog/10-things/10-physical-security-measures-every-organization-should-take/.
2371. Hudson K., Ruth A. , Microsoft Corporation, Securing Network Cabling, from http://flylib.com/books/en/2.902.1.22/1/.
2372. Mani Rathnam (Feb 1, 2015), Hardware Security, from http://www.slideshare.net/manirathnam39/hardware-security.
2373. Securing Network Devices, from
2374. http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+2+Securing+the+Network/Securing+Network+Devices/.
2375. Cisco CCNA Introduction to Security, from https://www.certificationkits.com/cisco-certification/cisco-ccna-640-802-exam certification-guide/cisco-ccna-introduction-to-security/.
2376. Irsandi Hasan (Sep 24, 2014), Network Fundamentals, from http://www.slideshare.net/kazhuyo/ccna-rsnb-chapter-11.
2377. Physical Security Handbook (April 2000), from http://download.cabledrum.net/wikileaks_archive/file/uscs-physical security-handbook.pdf.
2378. Security Awareness Training, from https://www.securityinnovation.com/training/information-security/physical-security training/.
2379. Laptop & Mobile Device Physical Security Dos & Don'ts!, from https://www.it.umass.edu/support/security/laptop-mobile device-physical-security-dos-donts.
2380. Physical Security “Dos” & “Don’ts” (September 9, 2014), from http://www.informationsecuritybuzz.com/news/physical security-dos-donts/.
2381. Faheem Ul Hasan (Nov 6, 2009), Physical Security Assessment, from http://www.slideshare.net/faheemi07/physical security-assessment.
2382. Davidcurriecia (Jan 5, 2009), Employee Security Awareness Program, from http://www.slideshare.net/davidcurriecia/Employee-Security-Awareness-Program.
2383. John Parmigiani, HIPAAs Security Regulations, from http://slideplayer.com/slide/683018/.
2384. Physical Security Audit Checklist (January 16, 2013), from http://locknet.com/lockbytes/excerpts/physical-security-audit checklist/.
2385. John Kirtland, from http://www.computerweekly.com/opinion/Challenges-and-benefits-of-physical-IT-security.
2386. Vijay Luiz(Aug 3, 2015), Physical security challenges when vendors are on site, from https://www.linkedin.com/pulse/physical-security-challenges-when-vendors-site-vijay-luiz.
2387. Understanding Security Layers, from http://www.slideshare.net/anoir2014/98-367-lesson-1-slides.
2388. E-Commerce: Security Challenges and Solutions, faculty.kfupm.edu.sa/COE/sadiq/richfiles/rich/ppt/security.ppt.
2389. Ztrace Gold, from http://www.ztrace.com/zTraceGold.asp.
2390. Prey, from http://preyproject.com.
2391. Absolute LoJack, from http://lojack.absolute.com/en.
2392. Laptopcop, from http://www.laptopcopsoftware.com.
2393. Gadgettrak, from http://www.gadgettrak.com.
2394. DellTM ProSupport Laptop Tracking & Recovery, from http://www.dell.com/content/topics/global.aspx/services/prosupport/computrace?c=us&l=en&cs=0.
2395. LocateMyLaptop, from http://locatemylaptop.com.
2396. TrackMyLaptop, from http://trackmylaptop.net.
2397. My Laptop Tracker, from http://www.mydevicetracker.com/laptop_tracking_software.asp.
2398. Locate Laptop Desktop Security, from http://www.unistal.com/laptop-tracker.html.
2399. Laptop Security Tool: EXO5, from http://www.exo5.com/.
2400. Ztrace Gold, from http://www.ztrace.com/zTraceGold.asp.
2401. Prey, from http://preyproject.com.
2402. Absolute LoJack, from http://lojack.absolute.com/en.
2403. Laptopcop, from http://www.laptopcopsoftware.com.
2404. Gadgettrak, from http://www.gadgettrak.com.

2405. DellTM ProSupport Laptop Tracking & Recovery, from http://www.dell.com/content/topics/global.aspx/services/prosupport/computrace?c=us&l=en&cs=0.
2406. LocateMyLaptop, from http://locatemylaptop.com.
2407. TrackMyLaptop, from http://trackmylaptop.net.
2408. My Laptop Tracker, from http://www.mydevicetracker.com/laptop_tracking_software.asp.
2409. Locate Laptop Desktop Security, from http://www.unistal.com/laptop-tracker.html.

APPENDIX C Virtual Private Network (VPN) Security

2410. P Raju (March 27th, 2013), Different Types of VPN Protocols, from http://techpp.com/2010/07/16/different-types-of-vpn protocols/
2411. VPN Consortium, January 2003, Definitions and Requirements, from http://www.hit.bme.hu/~jakab/edu/litr/VPN/vpn technologies.pdf.
2412. VPN Technologies, from http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html#vpn_tech.
2413. Firewalls and Virtual Private Networks, from http://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf.
2414. How the VPN Concentrator Works, from http://networkingtechnicalsupport.blogspot.in/2012/05/how-vpn-concentrator works.html.
2415. Cisco VPN Concentrator 3000, from http://www.nta-monitor.com/wiki/index.php/Cisco_VPN_Concentrator_3000.
2416. What is VPN Concentrator?, from http://wiki.answers.com/Q/What_is_VPN_Concentrator.
2417. Internetworking Fundamentals, http://www.orbit-computer-solutions.com/Remote-access-VPNs.php.
2418. JEFF TYSON & STEPHANIE CRAWFORD , How VPNs Work, from http://computer.howstuffworks.com/vpn3.htm.
2419. JEFF TYSON & STEPHANIE CRAWFORD , How VPNs Work, http://computer.howstuffworks.com/vpn4.htm.
2420. Chris Partsenidis, Hardware vs. software VPNs: Choose the right enterprise solution , from http://searchenterprisewan.techtarget.com/tip/Hardware-vs-software-VPNs-Choose-the-right-enterprise-solution.
2421. Martin Heller (Aug 8, 2006), What you need to know about VPN technologies, from http://www.computerworld.com/s/article/9002090/What_you_need_to_know_about_VPN_technologies.
2422. How Virtual Private Networks Work , from http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation ike-protocols/14106-how-vpn-works.html.
2423. Denial of Service Attack detection techniques, from https://www.evernote.com/shard/s9/note/b11a8c31-8651-4d74-acf9-1fb1b3c0f090/wishi/crazylazy#st=p&n=b11a8c31-8651-4d74-acf9-1fb1b3c0f090.
2424. SSL VPN Security, from http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html.
2425. SSL VPN (Secure Sockets Layer virtual private network), from searchsecurity.techtarget.com/definition/SSL-VPN.
2426. VLAN Trunking Protocol , from http://en.wikipedia.org/wiki/VLAN_Trunking_Protocol.
2427. What is VLAN Trunking Protocol (VTP) , from http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is vlan-trunking-protocol-vtp.php.
2428. VTP Version 2, from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html#wp1035121.
2429. VLAN Trunking Protocol (VTP), from http://etutorials.org/Networking/lan+switching/Chapter+8.+Virtual+LANs+VLANs/VLAN+Trunking+Protocol+VTP/.
2430. What is VLAN Trunking Protocol (VTP) Pruning , from http://www.omnisecu.com/cisco-certified-network-associate ccna/what-is-vlan-trunking-protocol-vtp-pruning.php.
2431. Configuring VTP, from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swvtp.pdf.
2432. Aaron (February 21, 2013), GRE over IPSec VPN Tunneling, from http://www.ccnpguide.com/gre-over-ipsec-vpn-tunneling/.
2433. Overview of GRE, from http://www.juniper.net/techpubs/en_US/junos12.1/topics/concept/gre-tunnel services.html#jd0e31
2434. 07/15/2016, How to configure a GRE tunnel, from https://supportforums.cisco.com/document/13576/how-configure-gre tunnel
2435. Mark Shea (Nov 12, 2010), How to Set Up VPN in Windows 7, from http://www.pcworld.com/article/210562/how_set_up_vpn_in_windows_7.html.
2436. FAHMIDA Y. RASHID (MAY 30, 2013), How to Set Up a VPN in Windows 7, from http://www.pcmag.com/article2/0,2817,2419612,00.asp.
2437. Fahmida Y. Rashid (03/06/2013), A guide to setting up a VPN in Windows 7, from http://www.itproportal.com/2013/06/03/a-guide-to-setting-up-a-vpn-in-windows-7/.
2438. Jeff Tyson, How Virtual Private Networks Work, from http://www.communicat.com/wp content/uploads/2013/04/how_vpn_work.pdf.
2439. Martin Heller (02 Oct 2006), 10 tips to secure client VPNs, from http://www.computerworld.com/s/article/9003779/10_tips_to_secure_client_VPNs?taxonomyId=16&pageNumber=1.
2440. (SEPTEMBER 11 2009), What Is VPN Encryption?, from http://www.thewhir.com/article-central/what-is-vpn-encryption.
2441. JEFF TYSON & STEPHANIE CRAWFORD, How VPNs Work, from http://computer.howstuffworks.com/vpn7.htm.
2442. Strong Authentication for SecureVPN Access Solving the Challenge of Simple and Secure Remote Access, from http://cacomvip.ca.com/fr/~/media/Files/whitepapers/strong-authentication-for-secure-vpn-access-wp.pdf.
2443. Azhar Shabbir Khan, Bilal Afzal BPLS VPNs with DiffServ – A QoS Performance study, from http://hh.diva portal.org/smash/get/diva2:400278/FULLTEXT01.pdf.

2444. QoS, from http://www.voip-info.org/wiki/view/QoS.
2445. Waheed Warden (2003-12-01), SSL VPN Deployment Considerations, from http://archive.networknewz.com/networknewz 10-20031201SSLVPNDeploymentConsiderations.html.
2446. Paul Ferguson, What Is a VPN? - Part I - The Internet Protocol Journal - Volume 1, No. 1, from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/what_is_a_vpn.html.
2447. FAHMIDA Y. RASHID (AUGUST 7, 2015), The Best Free VPN Services of 2015, from http://www.pcmag.com/article2/0,2817,2390381,00.asp.
2448. Alan Henry (3/20/14), What's The Best VPN Service Provider?, from http://lifehacker.com/whats-the-best-vpn-service provider-1547612561.
2449. Mike Bedford (22 Jun 16), The best free VPN services of 2016 in the UK, from http://www.pcadvisor.co.uk/features/internet/3497781/best-free-vpn-services-of-2014/.
2450. FIREWALLS, from http://mercury.webster.edu/aleshunas/COSC%205130/Chapter-22.pdf.
2451. February 2008, VPN SECURITY, from http://www.eetimes.com/document.asp?doc_id=1275828.
2452. Gabriel Knight June (26, 2013), Virtual Private Network: The Advantages of the VPN, from
2453. http://www.bandwidthplace.com/virtual-private-network-the-advantages-of-the-vpn-article/.
2454. Top 5 benefits using a VPN, from https://www.cactusvpn.com/vpn/top-5-benefits/.
2455. May 22, How the VPN Concentrator Works, from http://networkingtechnicalsupport.blogspot.in/2012/05/how-vpn concentrator-works.html.
2456. Cisco VPN Concentrator 3000, from http://www.nta-monitor.com/wiki/index.php/Cisco_VPN_Concentrator_3000.
2457. What is VPN Concentrator?, from http://wiki.answers.com/Q/What_is_VPN_Concentrator.
2458. Puneet Mehta, How does the VPN concentrator work?, from http://searchnetworking.techtarget.com/answer/How-does the-VPN-concentrator-work.
2459. Understanding the VPN 3000 Concentrator, from http://www.ciscomax.com/datasheets/VPN3000/Understanding%20the%20Cisco%20VPN%203000%20Concentrator.pdf.
2460. Concentrator NAT and PAT, from http://books.google.co.in/books?id=Qj3cDnFEezwC&pg=PA124&lpg=PA124&dq=functions+of+VPN+concentrator&source=
2461. bl&ots=wsPgwOT9SY&sig=2Tc7iIw1mVtcU lJWhW7DwGX6KQ&hl=en&sa=X&ei=bK0mVOadG4KNuAS4zoKAAQ&ved=0CBsQ6AEwADgU#v=onepage&q=functions%20of%20VPN%20concentrator&f=false.
2462. July 28, The Pros and Cons of Using a Virtual Private Network, from http://www.thrivenetworks.com/blog/2011/07/28/the pros-and-cons-of-using-a-virtual-private-network/.
2463. Lisa Phifer, What are the differences between a site-to-site VPN and a VPN client connecting to a VPN server?, from
2464. http://searchnetworking.techtarget.com/answer/What-are-the-differences-between-a-site-to-site-VPN-and-a-VPN-client connecting-to-a-VPN-server-Wh.
2465. CONFIGURING SITE TO SITE IPSEC VPN TUNNEL BETWEEN CISCO ROUTERS, from http://www.firewall.cx/cisco-technical knowledgebase/cisco-routers/867-cisco-router-site-to-site-ipsec-vpn.html.
2466. Sean Wilkins (MARCH 10, 2015), A Guide To Enterprise VPN Solutions, from http://www.tomsitpro.com/articles/enterprise vpn-solutions,2-885-2.html.
2467. Introducing additional Nokia Security (Nokia IP VPN), from https://books.google.co.in/books?id=IEeR9s4gL2oC&pg=PA23&lpg=PA23&dq=nokia+VPN+products&source=bl&ots=6UZnXE69aY&sig=ge9AmKlWA2bA-lk-8O23oh-INdo&hl=en&sa=X&ved=0ahUKEwir0-OR3brKAhXVB44KHbSGCU4Q6AEIRjAI#v=onepage&q=nokia%20VPN%20products&f=false.
2468. VPN Haus (Mar 20, 2012), SOME VPNS STILL FACE COMPATIBILITY, CONNECTION ISSUES , from http://vpnhaus.ncp e.com/2012/03/20/some-vpns-still-face-compatibility-connection-issues/.
2469. VPN Selection from, https://books.google.co.in/books?id=4YvNBQAAQBAJ&pg=PA212&lpg=PA212&dq=factors+considered+in+selecting+appropriate+VPN&source=bl&ots=JZj8MW6hKt&sig=AmBFl6T1ZHGlQcFU983Yh6H6w6I&hl=en&sa=X&ved=0ahUKEwjXtZ_ZxrzKAhVSA44KHUB4BYkQ6AEIOjAF#v=onepage&q=factors%20considered%20in%20selecting%20appropriate%20VPN&f=false.
2470. February 20, 2015, How to Choose a VPN Provider?, from https://privatoria.net/blog/how-to-choose-a-vpn-provider/.
2471. How to Choose the Best VPN Service for Your Needs, from http://www.howtogeek.com/221929/how-to-choose-the-best vpn-service-for-your-needs/.
2472. December 13, 2012, 5 things to look for when choosing a VPN Provider, from https://vpnreviewer.com/5-things-to-look when-choosing-vpn-provider.
2473. Karen Scarfone, Four criteria for selecting the right SSL VPN products, from http://searchsecurity.techtarget.com/feature/Four-criteria-for-selecting-the-right-SSL-VPN-products.
2474. VPN Tunneling, from http://compnetworking.about.com/od/vpn/a/vpn_tunneling.htm.
2475. VPN Consortium, January 2003, VPN Technologies: Definitions and Requirements, from http://www.hit.bme.hu/~jakab/edu/litr/VPN/vpn-technologies.pdf .
2476. Andrew Tarantola (3/26/13), VPNs: What They Do, How They Work, and Why You're Dumb for Not Using One, from http://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one.
2477. ENIGMAX (APRIL 15, 2012), How To Make VPNs Even More Secure, from https://torrentfreak.com/how-to-make-vpns even-more-secure-120419/.

2478. WHAT IS VPN TUNNELING?, from https://www.ivpn.net/what-is-a-tunnel
2479. Usman Javaid on December 02, 2011, What Is VPN & Tunneling; How To Create And Connect To VPN Network [Beginner's Guide], from http://www.addictivetips.com/windows-tips/what-is-vpn-how-to-create-and-connect-to-vpn-network/.
2480. WHAT IS VPN TUNNELING?, from http://www.dslreports.com/faq/5318.
2481. Virtual private network, from http://en.wikipedia.org/wiki/Virtual_private_network.
2482. Tunneling protocol , from http://en.wikipedia.org/wiki/Tunneling_protoco.l
2483. Margaret Rouse, tunneling or port forwarding, from http://searchenterprisewan.techtarget.com/definition/tunneling.
2484. Definition of: tunneling protocol, from http://www.pcmag.com/encyclopedia/term/53236/tunneling-protocol.
2485. Networking - What are voluntary and compulsory tunnels?, from http://www.careerride.com/Networking-voluntary-and compulsory-tunnels.aspx.
2486. Tunneling, from http://www.tech-faq.com/tunneling.html.
2487. AN INTRODUCTION TO VPN TUNNEL (Nov 21, 2011), from http://www.vpntunnel.co/an-introduction-to-vpn-tunnel.
2488. PPTP, from http://www.techterms.com/definition/pptp.
2489. Windows Server 2003/2003 R2 Retired Content, from http://technet.microsoft.com/en-in/library/cc739465(v=ws.10).aspx.
2490. Point-to-Point Tunneling Protocol, from http://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol.
2491. Point-to-Point Protocol, from http://en.wikipedia.org/wiki/Point-to-Point_Protocol.
2492. Password Authentication Protocol, from http://en.wikipedia.org/wiki/Password_authentication_protocol.
2493. B. Lloyd, W. Simpson (October 1992), from http://tools.ietf.org/html/rfc1334#page-3.
2494. Abdulrahman Abdullah Alhajj , Abdulrahman Khalid Abumurad , Cryptanalysis of Microsoft's Point-to-Point.
2495. Tunneling Protocol (PPTP), from http://www.just.edu.jo/~tawalbeh/cpe542/project/r2.pdf
2496. PPTP - Point to Point Tunneling Protocol (June 25, 2016), from http://compnetworking.about.com/od/vpn/l/aa030103a.htm.
2497. K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn(July 1999), Point-to-Point Tunneling Protocol (PPTP), from http://www.ietf.org/rfc/rfc2637.txt.
2498. Layer 2 Tunneling Protocol, from http://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol.
2499. Layer Two Tunneling Protocol and Internet Protocol Security, from http://technet.microsoft.com/en us/library/cc958047.aspx.
2500. Layer 2 Tunnel Protocol, from http://www.optimumdata.com/shop/files/cisco/3600/3600_Layer_2_Tunnel_Protocol.pdf.
2501. W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter(August 1999), Layer Two Tunneling Protocol "L2TP", from https://www.ietf.org/rfc/rfc2661.txt.
2502. Secure Socket Tunneling Protocol, from http://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol .
2503. Ricky M. Magalhaes (17 April 2007), from http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/Secure Socket-Tunneling-Protocol.html .
2504. Virtual Private Network Topology , from https://bto.bluecoat.com/packetguide/9.2/deploytopos/vpn.htm.
2505. VPN network topologies, from http://pic.dhe.ibm.com/infocenter/tivihelp/v30r1/index.jsp?topic=%2Fcom.ibm.lfs_admin.doc_1.1%2Ftopics%2Ftask_vpn_topologies.htm.
2506. VPN Topologies Guide, from http://www.internet-computer-security.com/VPN-Guide/VPN-Topologies.html.
2507. Advantages and Disadvantages of Hub-and-Spoke Operations, from http://aviationknowledge.wikidot.com/aviation:advantages-and-disadvantages-of-hub-and-spoke-opera.
2508. Configuring IPCop Firewalls, from https://www.safaribooksonline.com/library/view/configuring-ipcop firewalls/9781904811367/ch03s06.html.
2509. VPN Topologies Guide , from http://www.internet-computer-security.com/VPN-Guide/VPN-Topologies.html.
2510. Penna Sparrow, Mesh Topology: Advantages and Disadvantages, from http://www.ianswer4u.com/2011/05/mesh topology-advantages-and.html#axzz3ElkXi5M9.
2511. Penna Sparrow, Star Topology: Advantages and Disadvantages, from http://www.ianswer4u.com/2011/05/star-topology advantages-and.html#axzz3ElkXi5M9.
2512. Roy Hills (17 January 2003), NTA MONITOR UDP BACKOFF PATTERN FINGERPRINTING WHITE PAPER, from http://www.filewatcher.com/p/ike-scan-1.9p0.tgz.1240159/share/doc/ike-scan/udp-backoff-fingerprinting-paper.txt.html.
2513. ike-scan – IPsec VPN Scanning, Fingerprinting and Testing Tool, November 20, 2008, from http://www.darknet.org.uk/2008/11/ike-scan-ipsec-vpn-scanning-fingerprinting-and-testing-tool/.
2514. February 2008, VPN SECURITY, from http://www.infosec.gov.hk/english/technical/files/vpn.pdf.
2515. Threat Free Tunneling: Securing the VPN Traffic, from http://www.cyberoam.com/downloads/Whitepaper/SecuringYourVPN.pdf.
2516. Virtual Private Network, from http://www.biohealthmatics.com/technologies/networks/vpn.aspx.
2517. Martin Heller, 10 tips to secure client VPNs, from http://www.computerworld.com/s/article/9003779/10_tips_to_secure_client_VPNs?taxonomyId=16&pageNumber=1.
2518. 28 FEBRUARY 2013, How to Set up an L2TP/IPsec VPN Server on Windows, from http://www.elastichosts.com/support/tutorials/windows-l2tpipsec-vpn-server/.

2519. Network Defense: Security and Vulnerability Assessment, from http://books.google.co.in/books?id=bRCij3idUZYC&pg=SA4-PA7&lpg=SA4-PA7&dq=PPP-SSH,+VPN&source=bl&ots=5bCyHitUZJ&sig=E8JIjncQZCw6qYAP7kShaoVj4-s&hl=en&sa=X&ei=6UkqVOGeApHJuASZ-ILYCw&ved=0CBsQ6AEwADgU#v=onepage&q=PPP-SSH%2C%20VPN&f=false.
2520. Jordan Sissel(5-11-2012), Disabling battery/power management in Ubuntu, from http://www.semicomplete.com/articles/ppp-over-ssh/ .
2521. 9-7-2013, Howto VPN PPP-SSH in OpenSuse 12.3, from https://forums.opensuse.org/showthread.php/488564-Howto-VPN PPP-SSH-in-OpenSuse-12-3 .
2522. PPP-SSH Benefits, from http://searchsecurity.techtarget.com/definition/RADIUS.
2523. 14-4-2005, Vpn and Radius, from http://www.studymode.com/essays/Vpn-And-Radius-53297.html.
2524. RADIUS, from http://en.wikipedia.org/wiki/RADIUS.
2525. David Davis(12-7-2006), The importance of an effective VPN security policy, from http://www.techrepublic.com/article/the-importance-of-an-effective-vpn-security-policy/.
2526. RADIUS Protocol and Components, from http://technet.microsoft.com/en-us/library/cc726017(v=ws.10).aspx .
2527. Ron Nutter(14-8-2006), Securing a network with RADIUS and a VPN, from https://vpncreative.net/2013/03/04/vpn-speed.
2528. Margaret Rouse, SSL VPN (Secure Sockets Layer virtual private network), from http://searchsecurity.techtarget.com/definition/SSL-VPN.
2529. Different ways to transfer large amounts of Data over VPN, from http://arstechnica.com/civis/viewtopic.php?t=225049.
2530. Brien Posey(8-5-2003), Fix the four biggest problems with VPN connections, from http://www.techrepublic.com/article/fix the-four-biggest-problems-with-vpn-connections/.
2531. Salvatore Salamone(31-7-2002), Get IT Done: VPN reliability and scalability, from http://www.techrepublic.com/article/get it-done-vpn-reliability-and-scalability/.
2532. Guideline for setting up a functional VPN, from http://www.wingate.com/resources/WG/VPN_Setup_Guide.pdf.
2533. 2005, Virtual Private Network (VPN), from ftp://ftp.hp.com/pub/networking/software/ProCurve-SR-VPN-Config-Guide.pdf.
2534. VPN Configuration Guide, from http://www.vpntracker.com/cms_components/media/vpnt/VPNT_Interop_Howtos/1101/CiscoASA.pdf
2535. VPN service, from https://www.privateinternetaccess.com.
2536. Torguard, from https://torguard.net/.
2537. IPvanish VPN, from https://www.ipvanish.com.
2538. Cyberghost VPN, from http://www.cyberghostvpn.com/en_us.
2539. Hotspot shield, from http://www.hotspotshield.com.
2540. Tunnelbear, from https://www.tunnelbear.com.
2541. Private tunnel, from https://www.privatetunnel.com.
2542. VPNreactor, from http://www.vpnreactor.com/.
2543. Proxpn, from https://proxpn.com.
2544. Vyprvpn, from http://www.goldenfrog.com/vyprvpn.
2545. Authentify Solutions, from http://www.authentify.com/2fav/.

APPENDIX D Endpoint Security - MAC Systems

2546. Find out which macOS your Mac is using, from https://support.apple.com/en-in/HT201260.
2547. macOS Sonoma, from https://www.apple.com/in/macos/sonoma/.
2548. What is macOS, from https://www.javatpoint.com/what-is-macos
2549. Jamie (14 Jan 2022), MacOS architecture, from https://sojamie.medium.com/macos-architecture-64014381d79f.
2550. Architecture and components of MacOS, from https://www.bartleby.com/subject/engineering/computer-science/concepts/macos.
2551. Yuebin Sun, macOS Security Framework and previous CVEs, from https://rekken.github.io/2020/02/26/macOS-Security-Framework-and-Previous-CVEs-EN/.
2552. Understanding Common Data Security Architecture, from https://flylib.com/books/en/4.395.1.88/1/.
2553. File System Basics, from https://developer.apple.com/library/archive/documentation/FileManagement/Conceptual/FileSystemProgrammingGuide/FileSystemOverview/FileSystemOverview.html.
2554. macOS Vulnerabilities, from https://macpaw.com/mac-security-guide#macos-vulnerabilities.
2555. Consider your security options for your Mac, from https://www.mcafee.com/blogs/internet-security/can-apple-macs-get-viruses/#:~:text=So%2C%20Macs%20can%20and%20do,from%20the%20latest%20malware%20threats.
2556. Protecting against malware in macOS, from https://support.apple.com/en-gb/guide/security/sec469d47bd8/web.
2557. Sharon Shea, address space layout randomization (ASLR), from https://www.techtarget.com/searchsecurity/definition/address-space-layout-randomization-ASLR.
2558. Safer browsing with Safari, from https://www.apple.com/eg/macos/security/.
2559. Address Space Layout Randomization Next Generation, from https://www.mdpi.com/2076-3417/9/14/2928.
2560. Address Space Layout Randomization, from https://docs.oracle.com/en/operating-systems/oracle-linux/6/security/ol_aslr_sec.html.

2561. Kernel Architecture Overview, from https://developer.apple.com/library/archive/documentation/Darwin/Conceptual/KernelProgramming/Architecture/Architecture.html.
2562. Secure Enclave, from https://support.apple.com/en-in/guide/security/sec59b0b31ff/web.
2563. Set firewall access for services and apps, from https://support.apple.com/en-in/guide/mac-help/mh34041/mac#:~:text=Set%20firewall%20access%20for%20services,may%20need%20to%20scroll%20down.)&text=Click%20Options.,disabled%2C%20first%20turn%20on%20Firewall.
2564. Change Firewall settings on Mac, from https://support.apple.com/en-in/guide/mac-help/mh11783/mac.
2565. How To Turn ON & Turn Off Firewall On Mac (MacOS Sonoma), from https://www.howtoisolve.com/mac-firewall/.
2566. Protecting against malware in macOS, from https://support.apple.com/en-in/guide/security/sec469d47bd8/web.
2567. How to access XProtect on Mac, from https://iboysoft.com/wiki/xprotect-mac.html#how-to-access-xprotect-on-mac.
2568. 09 Aug 2022, What is XProtect on Mac? Is it Enough to Keep your Mac Safe, from https://news.trendmicro.com/2022/08/09/what-is-xprotect-on-mac-is-it-enough-to-keep-your-mac-safe/.
2569. What is Keychain Access on Mac, from https://support.apple.com/en-in/guide/keychain-access/kyca1083/mac.
2570. Guide to securing and improving privacy on macOS, from https://github.com/drduh/macOS-Security-and-Privacy-Guide.
2571. Mark O'Neill (19 Sep 2022), What is FileVault on Your Mac & Why Would You Want to Use it, from https://www.groovypost.com/howto/filevault-mac-encryption/.
2572. Should I be using FileVault disk encryption, from https://moonlock.com/what-is-filevault#:~:text=In%20addition%2C%20FileVault%20uses%20full,combinations%20required%20to%20crack%20it.
2573. Derek Erwin (03 Aug 2015), 15 Mac-Hardening Security Tips to Protect Your Privacy, from https://www.intego.com/mac-security-blog/15-mac-hardening-security-tips-to-protect-your-privacy/.
2574. Back up your Mac with Time Machine, from https://support.apple.com/en-in/HT201250.
2575. Choose a backup disk and set encryption options on Mac, from https://support.apple.com/en-gb/guide/mac-help/mh11421/mac.
2576. How to use Time Machine to back up or restore your Mac , from https://www.ucl.ac.uk/isd/sites/isd/files/migrated-files/How_to_use_Time_Machine_to_back_up_or_restore_your_Mac.pdf.
2577. How to use Time Machine on Mac for backup and restore tasks, from https://setapp.com/how-to/how-to-use-time-machine.
2578. About Startup Security Utility on a Mac with the Apple T2 Security Chip, from https://support.apple.com/en-in/HT208198.
2579. How to Turn Off Secure Boot on Mac, from https://www.wikihow.com/Turn-Off-Secure-Boot-on-Mac#:~:text=Mac%20computers%20equipped%20with%20a,(MBR)%20on%20your%20computer.
2580. Disabling and Enabling System Integrity Protection, from https://developer.apple.com/documentation/security/disabling_and_enabling_system_integrity_protection.
2581. About System Integrity Protection on your Mac, from https://support.apple.com/en-in/102149.
2582. System integrity protection, from https://nordvpn.com/cybersecurity/glossary/system-integrity-protection/.
2583. How to Find Macs with SIP Disabled and Enable It, from https://www.kolide.com/features/checks/mac-system-integrity-protection.
2584. Connie Yang (11 Dec 2023), What Is SIP on Mac & How to Enable/Disable SIP on Mac, from https://iboysoft.com/wiki/sip-mac.html.
2585. Enabling/disabling System Integrity Protection in macOS, from https://www.r-studio.com/data_recovery_macintosh/System_Integrity_Protection.shtml.
2586. Turn on two-factor authentication for your Apple ID, from https://support.apple.com/en-in/HT204915#:~:text=On%20your%20Mac%3A%20choose%20Apple,and%20follow%20the%20onscreen%20instructions.
2587. Use two-factor authentication for Apple ID security on your Mac, from https://support.apple.com/en-in/guide/mac-help/mchl8bd4e9c2/mac.
2588. Health Care IT Consulting, from https://logmeonce.com/resources/2023/08/09/two-factor-authentication-mac/#:~:text=A%3A%20The%20main%20benefit%20of,is%20%E2%81%A3safe%20and%E2%80%8D%20secure.
2589. Apple Platform Security, from https://support.apple.com/en-in/guide/security/sec79afd0274/web.
2590. Use built-in network security features for Apple devices, from https://support.apple.com/en-in/guide/deployment/depb59c050ef/web.
2591. Prevent cross-site tracking in Safari on Mac, from https://support.apple.com/en-in/guide/safari/sfri40732/mac.
2592. How to use Safari's tools to protect your privacy while browsing, from https://www.theverge.com/2020/2/12/21124844/apple-mac-safari-privacy-tools-private-network-browser-settings.
2593. AirDrop operation, from https://support.apple.com/en-in/guide/security/sec2261183f4/web#:~:text=AirDrop%20uses%20iCloud%20services%20to,with%20the%20user's%20Apple%20ID.
2594. AirDrop security, from https://support.apple.com/en-in/guide/security/sec2261183f4/web.
2595. Use AirDrop on your Mac, from https://support.apple.com/en-in/102538.
2596. 24 Aug 2020, macOS Security: Managing Privileged Access & Credentials, from https://www.beyondtrust.com/blog/entry/macos-security-managing-privileged-access-credentials.
2597. Demystifying Mac Administration: Big Sur, Zero-Touch, and the Mac vs. PC at Work Debate, from https://jumpcloud.com/blog/demystifying-mac-administration-challenges-trends-2021.
2598. Change Users & Groups settings on Mac, from https://support.apple.com/en-in/guide/mac-help/mtusr001/mac.
2599. Kirk McElhearn (21 Sep 2023), Understanding User Accounts in macOS, from https://www.intego.com/mac-security-blog/understanding-user-accounts-in-macos/.

2600. How to Set Up Parental Control on Mac, from https://www.howtoisolve.com/how-apply-restriction-on-use-installed-mac-apps-os-x-yosemite/.
2601. Create a sharing-only user account on Mac, from https://support.apple.com/en-in/guide/mac-help/mchlp15577/mac#:~:text=If%20you%20want%20to%20give,Users%20%26%20Groups%20in%20the%20sidebar.
2602. Glenn Fleishman(27 May 2021), How to create a sharing-only user in macOS to limit access, from https://www.macworld.com/article/346628/create-a-sharing-only-user-in-macos-to-limit-access.html.
2603. Change Guest User settings on Mac, from https://support.apple.com/en-in/guide/mac-help/mh15600/mac#:~:text=Learn%20how%20to%20set%20up,can't%20select%20Guest%20User.
2604. Abbaz Uddin (02 Jun 2023), How to Create a Guest Account on a Mac, from https://www.maketecheasier.com/create-guest-account-mac/.
2605. Francis Yom, macOS Least Privilege Best Practices to Combat Rising Ransomware, from https://www.cyberark.com/resources/blog/macos-least-privilege-best-practices-to-combat-rising-ransomware.
2606. Tips for creating secure passwords on Mac, from https://support.apple.com/en-in/guide/mac-help/mchlp1088/mac.
2607. Recommended macOS Security Configurations, from https://support.addigy.com/hc/en-us/articles/4403726652435-Recommended-macOS-Security-Configurations.
2608. Information Security Strategies for macOS Devices, from https://informationsecurity.wustl.edu/guidance/information-security-strategies-for-macos-devices/.
2609. Encrypt and protect a storage device with a password in Disk Utility on Mac, from https://support.apple.com/en-in/guide/disk-utility/dskutl35612/mac.
2610. Dany (28 Nov 2023), How to Encrypt Hard Drive on a Mac with 2 Reliable Methods, from https://www.easeus.com/computer-instruction/encrypt-hard-drive-mac.html.
2611. How to encrypt a Mac storage device, from https://www.macworld.com/article/344206/how-to-encrypt-a-mac-storage-device.html.
2612. How to encrypt an external USB drive using Disk Utility in MacOS, from https://www.douglascollege.ca/sites/default/files/docs/student-services/How%20to%20Encrypt%20an%20external%20USB%20drive%20using%20Disk%20Utility%20in%20macOS.pdf.
2613. Unlocking passwordless Mac authentication, from https://www.jamf.com/blog/unlocking-passwordless-mac-authentication/.
2614. Use security keys for two-factor authentication on Mac, from https://support.apple.com/en-in/guide/mac-help/mchld6920426/mac.
2615. Anus Fox (03 Oct 2023), A security policy for macOS Sonoma, from https://www.linkedin.com/pulse/security-policy-macos-sonoma-angus-fox/.
2616. How to disable account on OS X Mavericks, from https://apple.stackexchange.com/questions/135184/how-to-disable-account-on-os-x-mavericks.
2617. How can I disable a User Account from the CLI with Mac OS X Server, from https://serverfault.com/questions/61214/how-can-i-disable-a-user-account-from-the-cli-with-mac-os-x-server#new-answer.
2618. Change permissions for files, folders or disks on Mac, from https://support.apple.com/en-in/guide/mac-help/mchlp1203/mac.
2619. Configure a Gatekeeper setting in Apple Business Essentials, from https://support.apple.com/en-in/guide/apple-business-essentials/axmd2430181c/web.
2620. Open apps safely on your Mac, from https://support.apple.com/en-in/HT202491.
2621. View information about Mac processes in Activity Monitor, from https://support.apple.com/en-in/guide/activity-monitor/actmntr1001/mac.
2622. Set a firmware password on your Mac, from https://support.apple.com/en-in/HT204455.
2623. Change Sharing settings on Mac, from https://support.apple.com/en-in/guide/mac-help/mchl26e04309/mac#:~:text=On%20your%20Mac%2C%20use%20Sharing,may%20need%20to%20scroll%20down.).
2624. Change Media Sharing settings on Mac, from https://support.apple.com/en-in/guide/mac-help/hspe13371337/mac.
2625. Danny Maiorca (27 Jan 2023), How to Change Your Mac Sharing Settings, from https://appletoolbox.com/how-to-change-your-mac-sharing-settings/.
2626. Set a firmware password on your Mac, from https://support.apple.com/en-in/HT204455.
2627. Azwan Jamaluddin (31 Aug 2023), How to Make Your Mac More Secure with a Firmware Password, from https://www.hongkiat.com/blog/secure-mac-firmware-password/.
2628. Daisy, How to Turn On/off Firmware Password on Mac, from https://www.easeus.com/computer-instruction/turn-off-firmware-password-on-mac.html.
2629. Disable Remote Management, from https://www.tenable.com/audits/items/CIS_Apple_macOS_11_v1.2.0_L1.audit:db78ec0a309ad050edcf25c2ce2683f0.
2630. Enable remote management for Remote Desktop, from https://support.apple.com/en-in/guide/remote-desktop/apd8b1c65bd/mac.
2631. How to Disable Remote Management using Mac Terminal, from https://code2care.org/howto/disable-remote-management-using-mac-terminal/?un=1.
2632. Emma Collins (04 May 2023), Remote Management for Apple Devices, from https://www.helpwire.app/blog/mac-remote-management/
2633. Sandy Writtenhouse (16 Jun 2023), How to stop Safari on Mac from automatically opening web downloads, from https://www.idownloadblog.com/2019/07/10/stop-opening-downloads-safari-mac/.
2634. HOW TO PREVENT SAFARI ON YOUR MAC FROM AUTOMATICALLY OPENING DOWNLOADED FILES, from https://www.easytech.lu/blog/macos-tip-prevent-safari-from-opening-downloaded-files.
2635. Protecting against malware in macOS, from https://support.apple.com/en-in/guide/security/sec469d47bd8/web.
2636. Protect your Mac from malware, from https://support.apple.com/en-in/guide/mac-help/mh40596/mac.

2637. How to allow install of non app store or identified developers on MacOS Sierra, from https://apple.stackexchange.com/questions/294013/how-to-allow-install-of-non-app-store-or-identified-developers-on-macos-sierra.
2638. Change Wi-Fi settings on Mac, from https://support.apple.com/en-in/guide/mac-help/mh11935/mac.
2639. Lory Gil (28 Feb 2018), How to stop auto-joining a wifi network on Mac in High Sierra, from https://www.imore.com/how-stop-auto-joining-wifi-network-mac
2640. Install and uninstall apps from the internet or a disc on Mac, from https://support.apple.com/en-in/guide/mac-help/mh35835/mac.
2641. Uninstall apps on your Mac, from https://support.apple.com/en-us/102610
2642. Require a password after waking your Mac, from https://support.apple.com/en-in/guide/mac-help/mchlp2270/mac#:~:text=On%20your%20Mac%2C%20choose%20Apple,may%20need%20to%20scroll%20down.)&text=Click%20the%20pop%2Dup%20menu,before%20a%20password%20is%20required.
2643. Lee Stanton (05 Sep 2023), How To Set A Screensaver On A Mac, from https://www.alphr.com/set-screensaver-mac/.
2644. Search with Spotlight on Mac,from https://support.apple.com/en-in/guide/mac-help/mchlp1008/mac#:~:text=Spotlight%20can%20help%20you%20quickly,calculations%20and%20conversions%20for%20you.
2645. Turn off Siri Suggestions for Spotlight on Mac, from https://support.apple.com/en-in/guide/mac-help/mchl62db64f5/mac.
2646. How to Turn Off Siri Suggestions, from https://botpenguin.com/how-to-turn-off-siri-suggestions/
2647. Lock devices, from https://support.apple.com/en-in/guide/deployment/depb980a0be4/web#:~:text=Lock%20a%20Mac%3A%20Mobile%20device,and%20validated%20by%20the%20Mac.
2648. Wipe for macOS devices,from https://www.miradore.com/knowledge/macos/wipe-for-macos-devices/#:~:text=The%20wipe%20is%20a%20security,device%20with%20ease%20when%20required.
2649. Use MDM to enable Remote Management in macOS, from https://support.apple.com/en-in/102024.
2650. Erase Apple devices,from https://support.apple.com/en-in/guide/deployment/dep0a819891e/web.
2651. Locking a Mac remotely, from https://www.miradore.com/knowledge/macos/locking-mac-remotely/
2652. Smriti (24 Apr 2023), Wipe all data from a macOS device, from https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-wipe-macos.
2653. Remote Lock and Remote Wipe with Addigy Mobile Device Management (MDM), from https://support.addigy.com/hc/en-us/articles/4403542406419-Remote-Lock-and-Remote-Wipe-with-Addigy-Mobile-Device-Management-MDM-
2654. Block connections to your Mac with a firewall, from https://support.apple.com/en-in/guide/mac-help/mh34041/mac.
2655. Change Firewall settings on Mac, from https://support.apple.com/en-in/guide/mac-help/mh11783/14.0/mac/14.0.
2656. Ratnesh Kumar (04 Sep 2023), How to Enable and Use Firewall on Mac in macOS 14 Sonoma, from https://geekchamp.com/how-to-enable-and-use-firewall-on-mac/.
2657. How Do I Open Firewall Ports for Apple Mac, from https://www.techsolutions.support.com/how-to/how-do-i-open-firewall-ports-for-apple-mac-11403.
2658. Use SSL to connect to the outgoing mail server in Mail on Mac, from https://support.apple.com/en-in/guide/mail/mlhlp1072/mac.
2659. How to Use SSL With an Email Account in macOS Mail, from https://www.lifewire.com/os-x-ssl-email-1165001.
2660. Set up a VLAN on Mac, from https://support.apple.com/en-in/guide/mac-help/mh15134/mac.
2661. How to setup VLAN from Mac OS Mojave using terminal, from https://superuser.com/questions/1535964/how-to-setup-vlan-from-mac-os-mojave-using-terminal.
2662. Apple Remote Desktop User Guide, from https://support.apple.com/en-in/guide/remote-desktop/welcome/mac.
2663. Using RDP to Connect to a Windows Computer from MacOS, from https://cat.pdx.edu/platforms/mac/remote-access/using-rdp-to-connect-to-a-windows-computer-from-macos/.
2664. Temporarily allow a website to see your IP address in Safari on Mac, from https://support.apple.com/en-hk/guide/safari/ibrwc3feb013/mac.
2665. Use iCloud Private Relay on Mac, from https://support.apple.com/en-in/guide/mac-help/mchlecadabe0/mac.
2666. Cassie (24 Oct 2023), How to Turn On/Off Automatic Updates on macOS Sonoma/Ventura, from https://www.drbuho.com/how-to/turn-on-automatic-updates-mac.
2667. Keep your Mac up to date, from https://support.apple.com/en-in/guide/mac-help/mchlpx1065/mac.
2668. What is Mac patch management, from https://www.kandji.io/apple-mdm-definitions/what-is-mac-patch-management/#:~:text=Mac%20patch%20management%20refers%20to,to%20date%20through%20periodic%20updates.
2669. Patch Management for macOS devices, from https://www.manageengine.com/patch-management/mac-patch-management.html#:~:text=Mac%20patch%20management%20involves%20managing,the%20production%20environment%20for%20deployment.
2670. Vivek Gite (27 Oct 2023), How To Update macOS Using Command Line Software Update Tool, from https://www.cyberciti.biz/faq/apple-mac-os-x-update-softwareupdate-bash-shell-command/.
2671. Kelsey Kinzer(14 Mar 2022), Key Considerations for macOS Patch Management, from https://jumpcloud.com/blog/macos-patch-management.
2672. Jimmy Graham (14 Aug 2019), Optimizing the patch management process, from https://www.helpnetsecurity.com/2019/08/14/patch-management-process/.
2673. Automated Patch Management Tool, from https://www.solarwinds.com/patch-manager/use-cases/automated-patch-management
2674. Cristian Neagu, Patch Management Policy, from https://heimdalsecurity.com/blog/patch-management-policy/.

References

2675. Omkar Hiremath, BASICS OF PATCH MANAGEMENT POLICIES, from https://www.softwaresecured.com/basics-of-patch-management-policies/.

2676. Create a MacOS Patch Policy, from https://jumpcloud.com/support/create-a-macos-patch-policy.

2677. Deploy patches automatically with Automated Patch Management Software, from https://www.manageengine.com/patch-management/automated-patch-deployment.html?fea_drop.

2678. Endpoint automation to propel your digital workplace, from https://www.manageengine.com/products/desktop-central/.

2679. What is Patch Manager Plus, from https://www.manageengine.com/patch-management/.

2680. Patch & Asset Management, from https://heimdalsecurity.com/enterprise-security/products/patch-management-software.

2681. Simplify Mac patch management, from https://www.ninjaone.com/patch-management/macos/.

2682. Patching fit for any business need, from https://lp.atera.com/patch-management.

2683. Patch Management, from https://jumpcloud.com/platform/patch-management.